Homeland Defense Command & Control (HLD C2) FY02 ACTD Proposal

July 2001

Mr. Don Eddington
DISA AITS-JPO
703-284-8881
eddingtd@aits-jpo.disa.mil

Maj Mike Malone, USMC
USJFCOM J02M
757-836-0217
malonem@jfcom.mil

Objectives of Homeland Defense C2 ACTD

- Demonstrate **new concepts for command and control**
  - *for warning and coordination of escalating defense of the U.S. against unconventional threats*
  - *among DoD and its partners (federal, state, local, private)*
  - *concepts that will work regardless of the organizational outcome of the HLD evolution*
- Demonstrate key technologies that will **assure the integrity of C2 and situational awareness**
  - *during periods of intense disruption to homeland infrastructure*

Homeland Security - Definitions

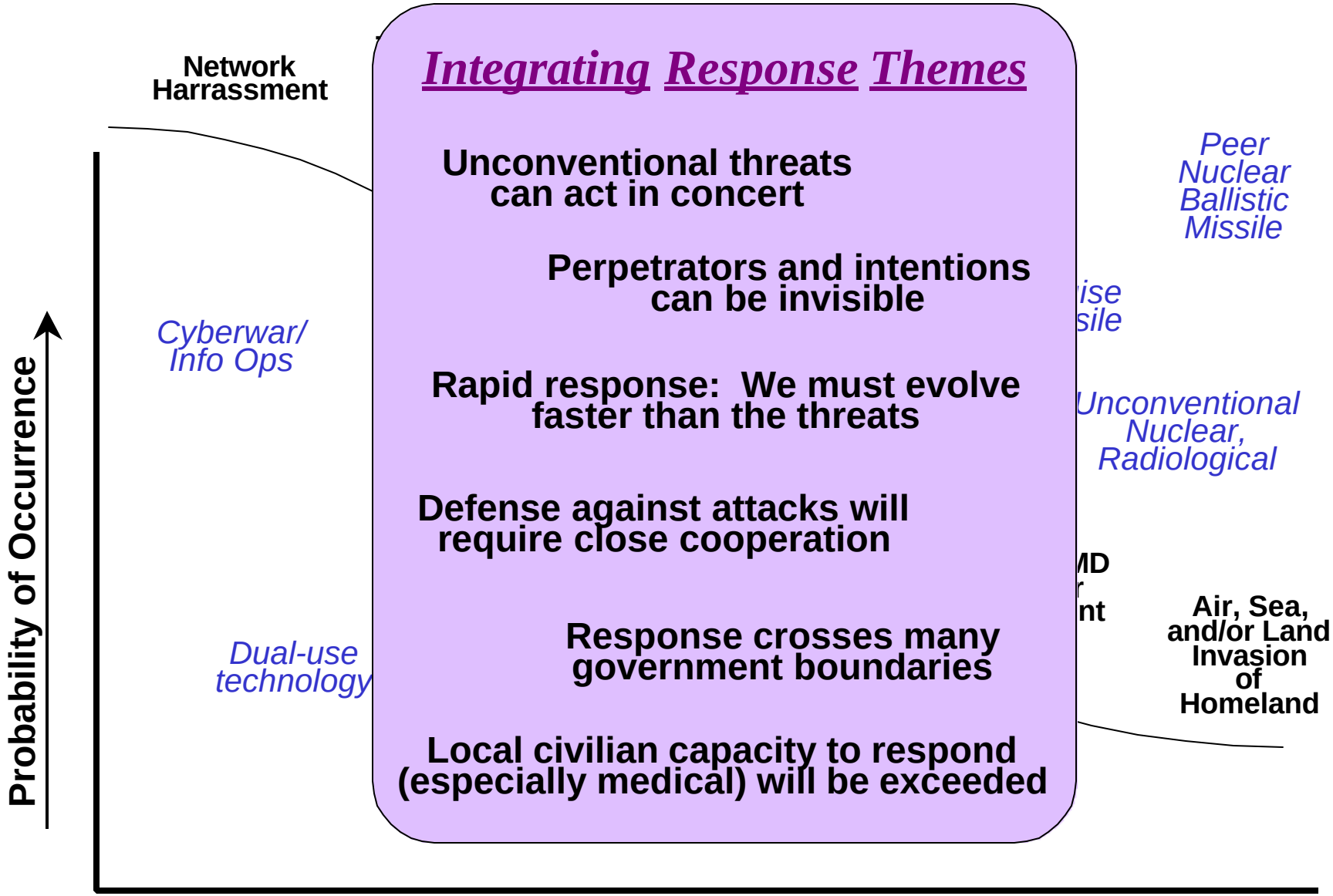
- **Homeland Security:** "the prevention, deterrence, and preemption of, and defense against aggression targeted at U.S. territory, sovereignty, population, and infrastructure as well as the management of the consequences of such aggression and other domestic emergencies" ***It includes . . .***
- **Homeland* Defense:** "the prevention, deterrence, preemption of, and defense against direct attacks aimed at U.S. territory, population, and infrastructure"
- **Civil Support:** "DoD support to civilian authorities for natural and manmade domestic emergencies, civil disturbances, and designated law enforcement efforts"

QDR team definition

* *For DoD, homeland includes Canada & U.S. territories*

Threats and Vulnerabilities

Likelihood of Threats to Homeland*



250,000-300,000 terrorist acts against Americans in past 20 years

* CONUS, Alaska, Hawaii, Canada

Homeland Defense Vulnerabilities

- **Non-interoperable DoD, government, civilian systems**
- **Complex technical, policy, legal interagency coordination issues**
- **DoD reliance on civilian/commercial infrastructure**
- **Internet (superb C2 system) relies on 13 "key" nodes**
- **> 22K cyber attacks on DoD systems in '99, > 23K in first half of '01**
  - *"I Love You" virus contaminated over 1 million computers in 5 hours*
- **National health care system at 95% capacity**
- **Ineffective early BW threat assessment capability**
- **Widespread availability & low cost of NBC & information technology**
  - *Russian BW program created enough anthrax to kill world's population four times over. $250K investment can produce anthrax simulant in 3 weeks*
  - *1500 tons nuclear material in Russia*

Defense Science Board 2000 Summer Study, "Protecting the Homeland", Feb 2001

The Politics

Numerous Approaches to HLD Management

- Create National Homeland Security Agency
- Give National Guard the lead, with Reserves in support
- Create a "CINC Americas / HLD Command"
- Structure active forces around one MRC plus HLD/LRCs

But three themes remain consistent across management schemes:

- Overall C2 must be "coordinated" across 40+ agencies
  - *need integrated warning / information / coordination system*
- 7 CINCs may be involved in response to HLD threats
- Responsibilities should be allocated as:
  - ***Federal*** *- deterrence, prevention, preemption, attribution, retaliation*
  - ***State / Local*** *- first response, consequence management*
  - ***Private Sector*** *- defense & response to cyber & biological attack*

Concepts of Operations to fit any of the options

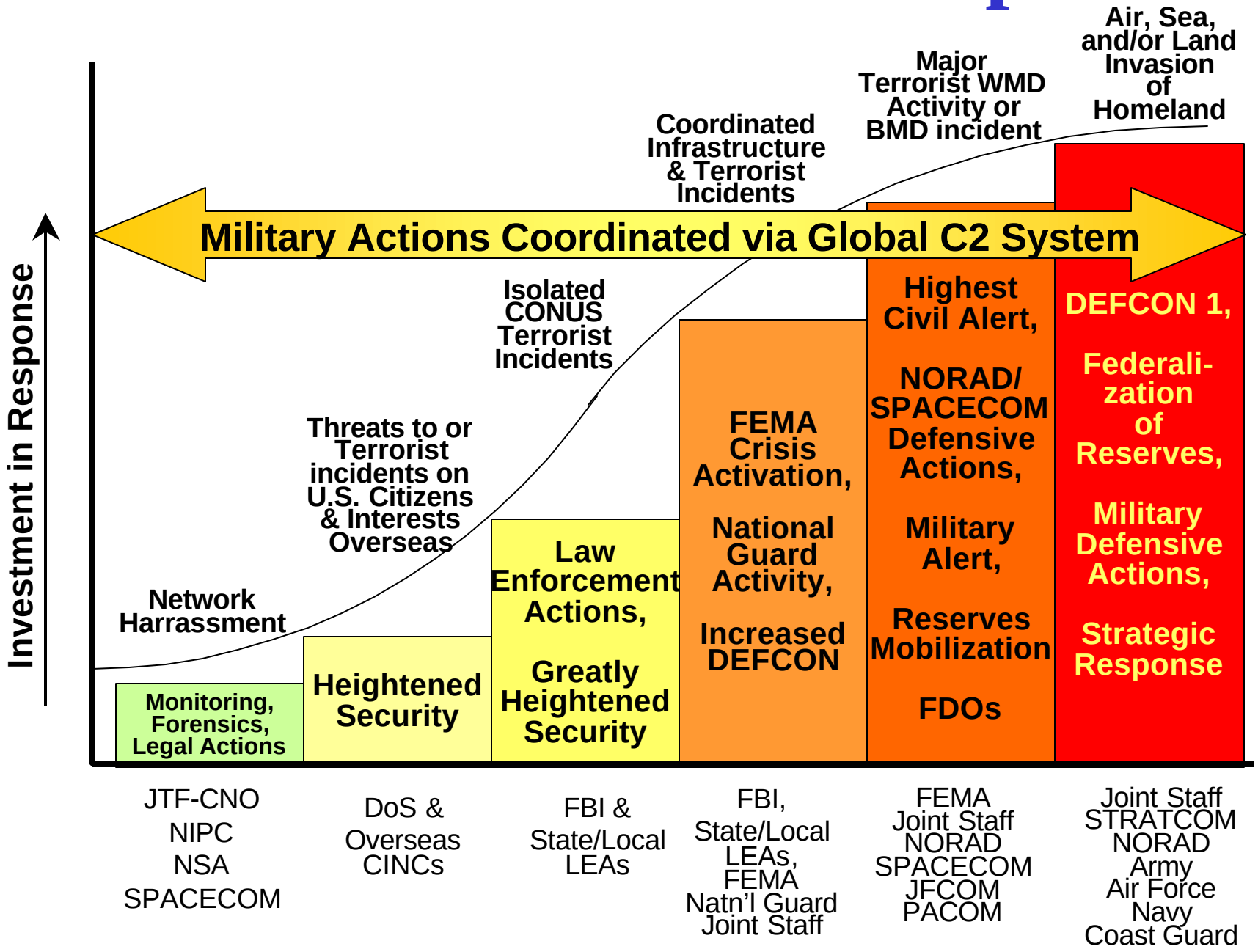
Homeland Defense C2

What are possible new C2 Concepts?

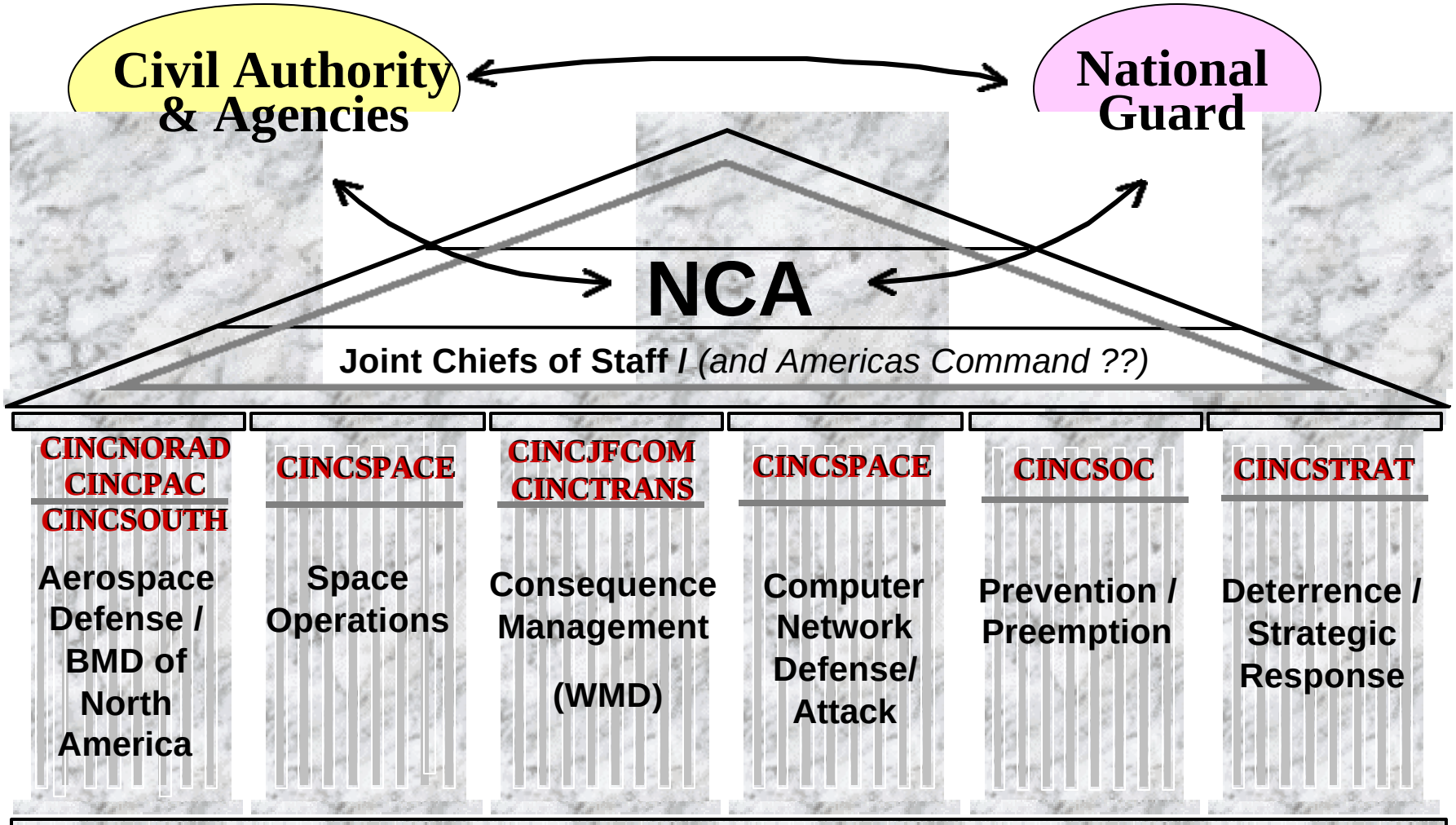
- **Coordination of concurrent operations between <u>multiple</u> supported CINCs and agencies …..**
  - *parallel operations, "composite warfare command"*
    - *analogous to Federal Response Plan for disaster relief*
  - *CONOPs for various degrees of conflict and infrastructure disruption*
    - *DoD in a supporting role to civilian agencies in some areas, and a lead role in others*
  - *intelligence coordination across dissimilar domains*
- **Significant reliance on the commercial infra-structure** (where <u>most</u> of the players reside, including local incident personnel), augmented by a **HLD core* in the DoD Global Information Grid**

** We'll get to the new technology in a few minutes . . .*

Homeland Defensive Response

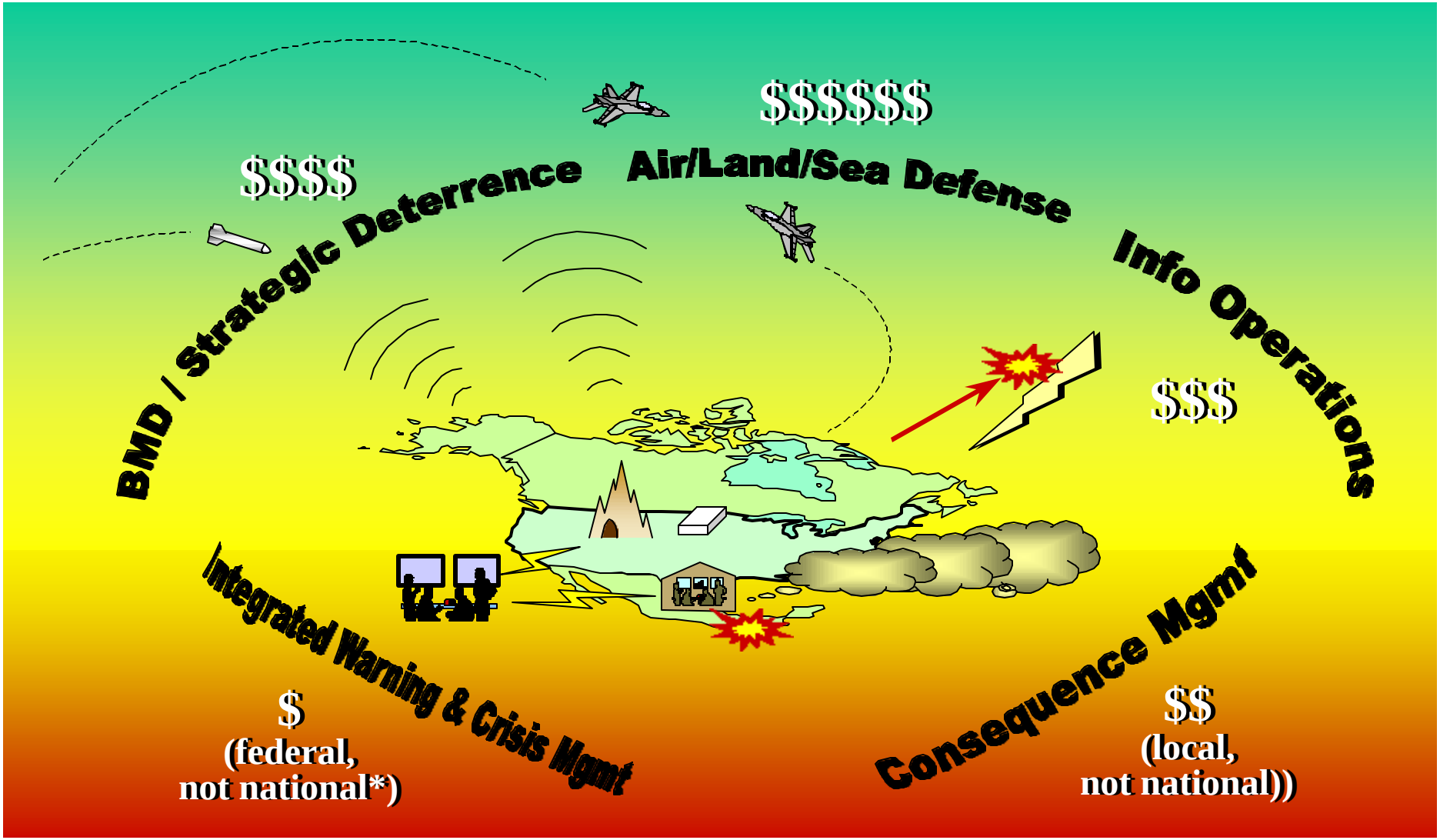


DoD Federated HLD C2 Framework



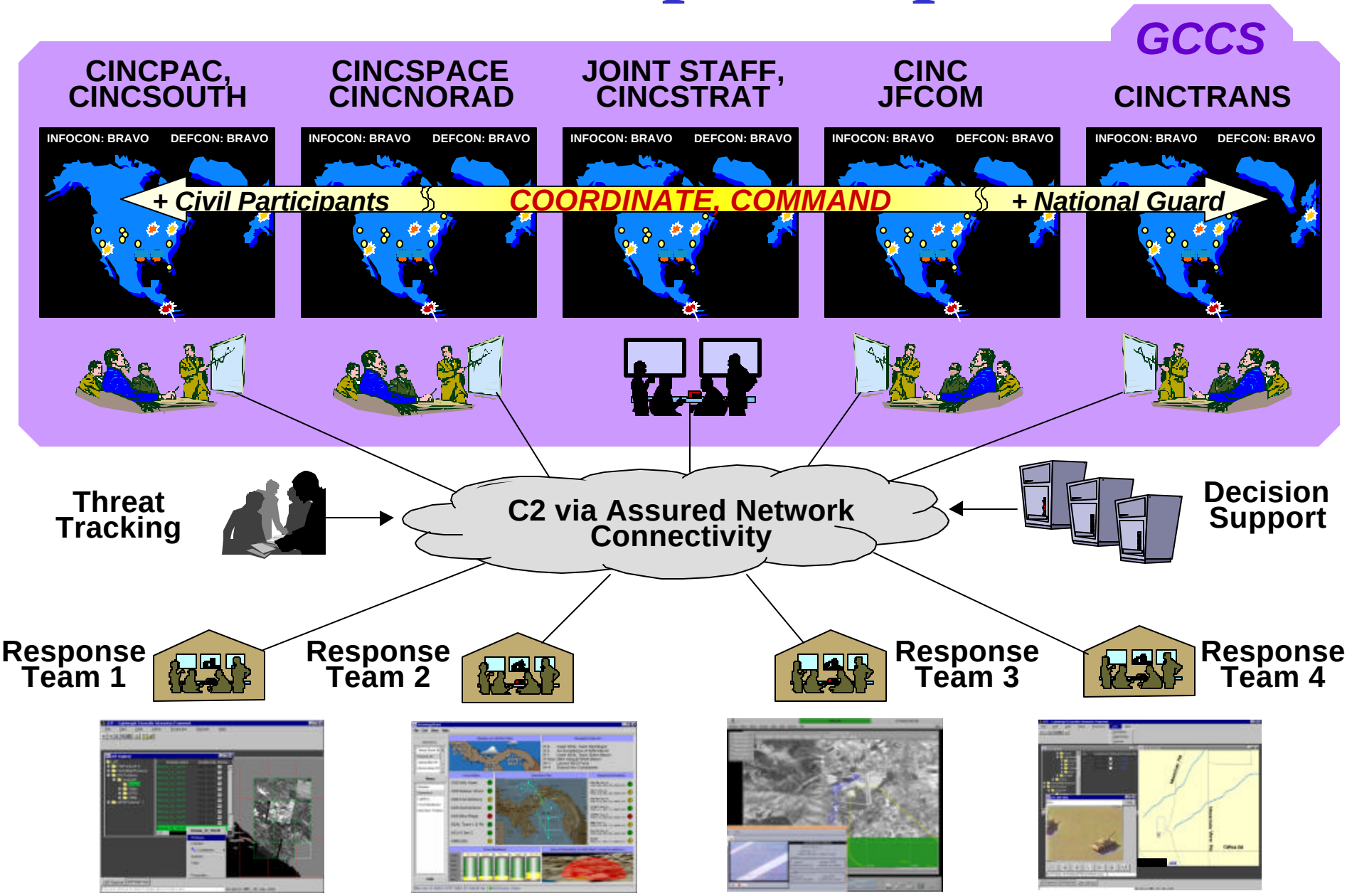
- Command and Control
- Common Battlespace Picture
- On-Demand, Precise, Decision-Quality Information
- Early Capability Assessment (predictive or I&W)
- Attack Prevention thru Deterrence or Interdiction
- Protection of Critical Assets & Infrastructure
- Attribution of Perpetrators and Retaliation (chains of evidence)

Status of DoD's response capability

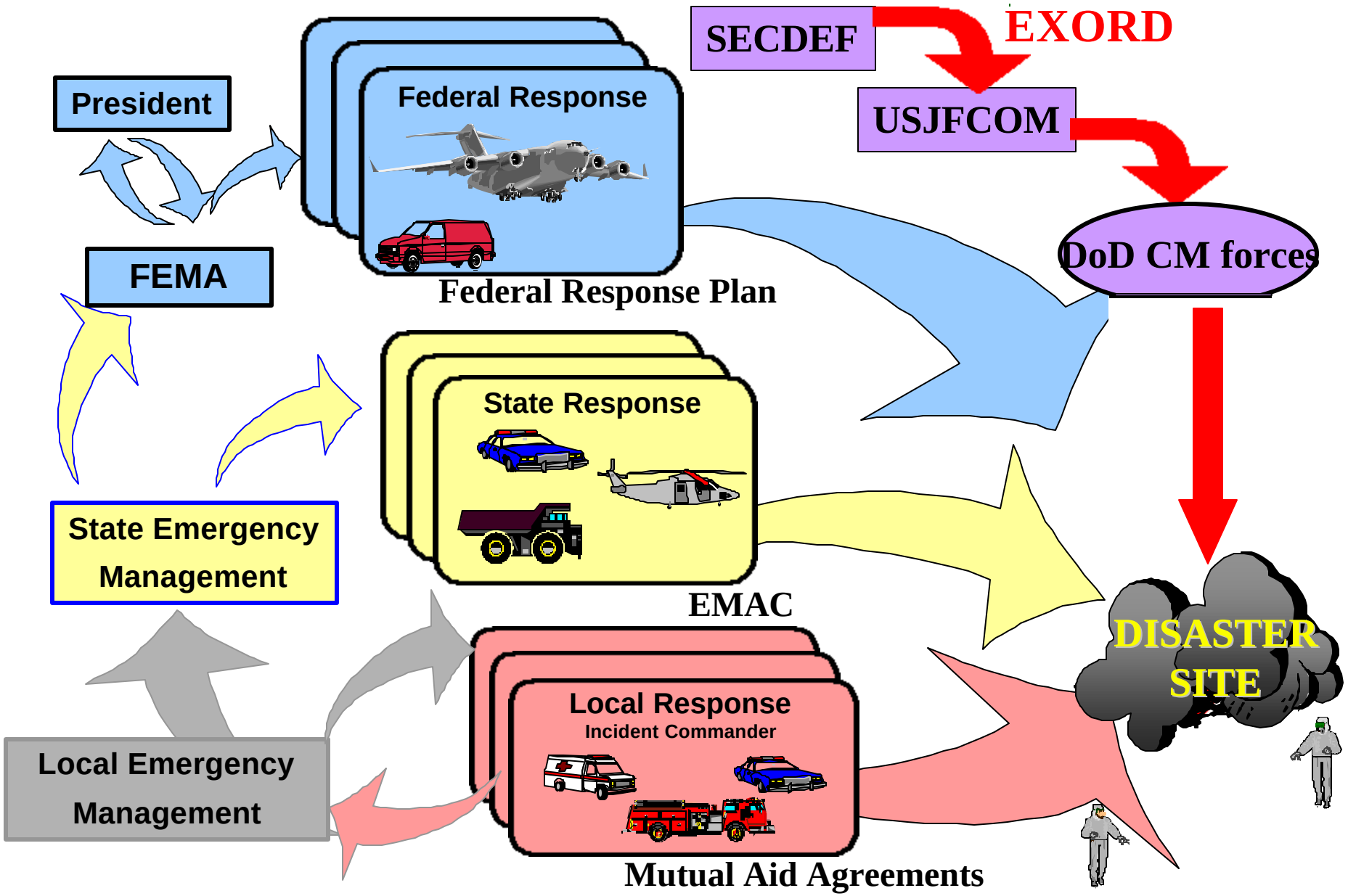


** national = federal + state (incl nat'l guard) + local*

HLD C2 Concept of Operations



Analogous Distributed CONOPS for Disaster Response



The Technologies

Critical Capabilities for Homeland Defense C2

- **We do not plan to take on either the full breadth of Homeland Defense or a wide variety of technologies**
  - **there is a lot of money focused at BMD, U.S. Air Defense, & Force deployment coordination**

- **We intend to focus on <u>three</u> <u>key</u> <u>technology areas</u> in which risk must be reduced before an integrated C2 capability for Homeland (or global) defense can be constructed**

Three Critical Capabilities for Homeland Defense C2

- **ASSURED CONNECTIVITY: Situation assessment and coordination across National Command and the CINCs, Services, Agencies, Departments, States, Law Enforcement, etc during high network disruption**

- **ATTRIBUTION: Capability to assess and track the threat across multiple information domains; and provide high-confidence, timely alerts**

- **CRISIS COORDINATION -- *FIRST RESPONSE THROUGH CONSEQUENCE MGMT*: Provide coordinated response to contain/ neutralize threats and recover from damage**

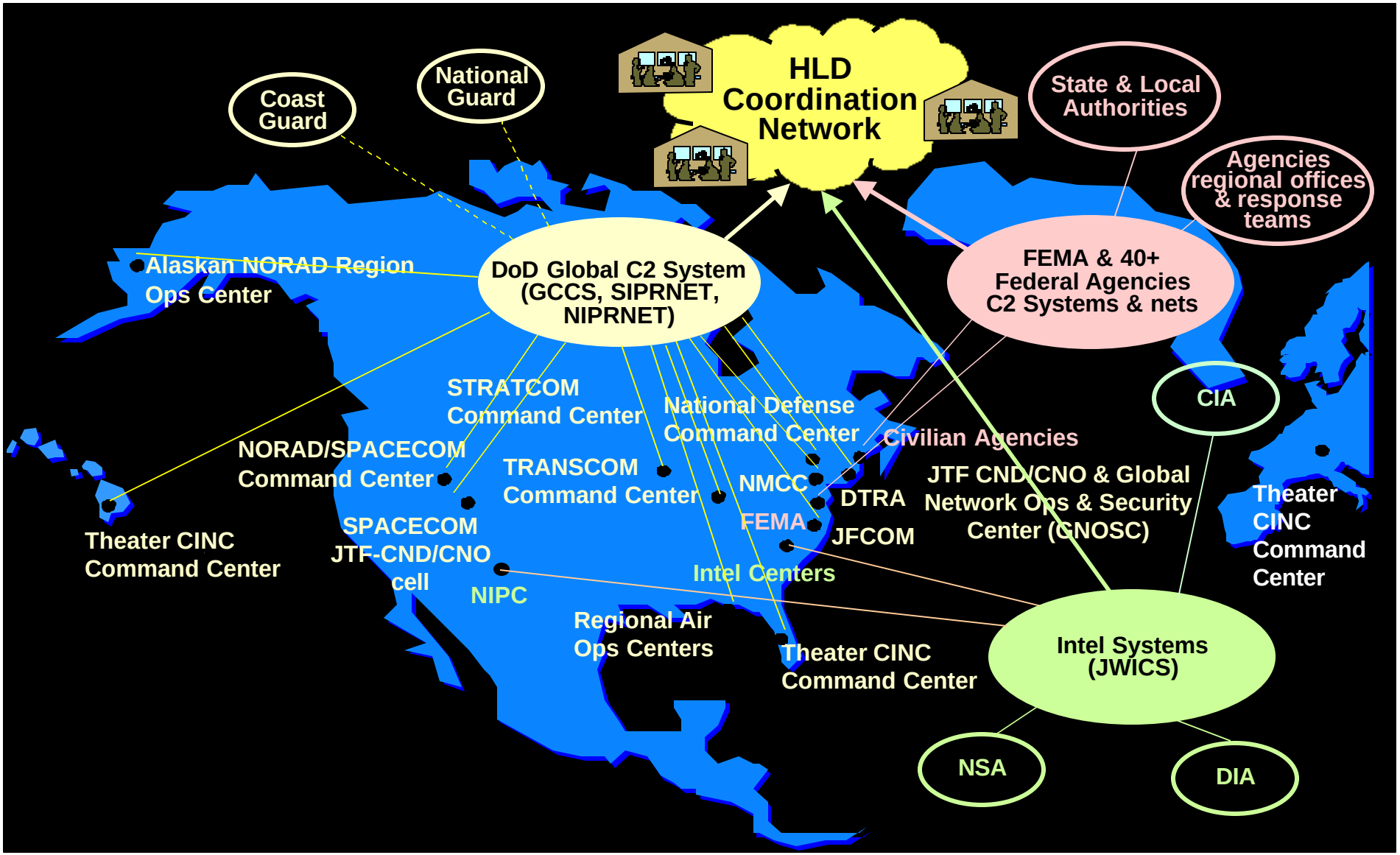
First Critical Capability

- **<u>ASSURED CONNECTIVITY:</u> Situation assessment and coordination across National Command and the CINCs, Services, Agencies, Departments, States, Law Enforcement, etc during high network disruption**

- **Enabling Technology Areas**
  - a **secure, survivable inter-agency coordination network**
    - *built <u>through</u> the commercial infrastructure*
    - *with **military network augmentation (GIG*)** as needed to ensure availability.*
  - **Dynamic, assured quality of service** data, voice, video, multimedia conferencing & streaming data for disadvantaged & mobile users
  - **Defense-in-Depth and redundant failover** options for the National and Defense Information Infrastructures (NII, DII/GIG)

* *Survivable subnet of the Global Information Grid*

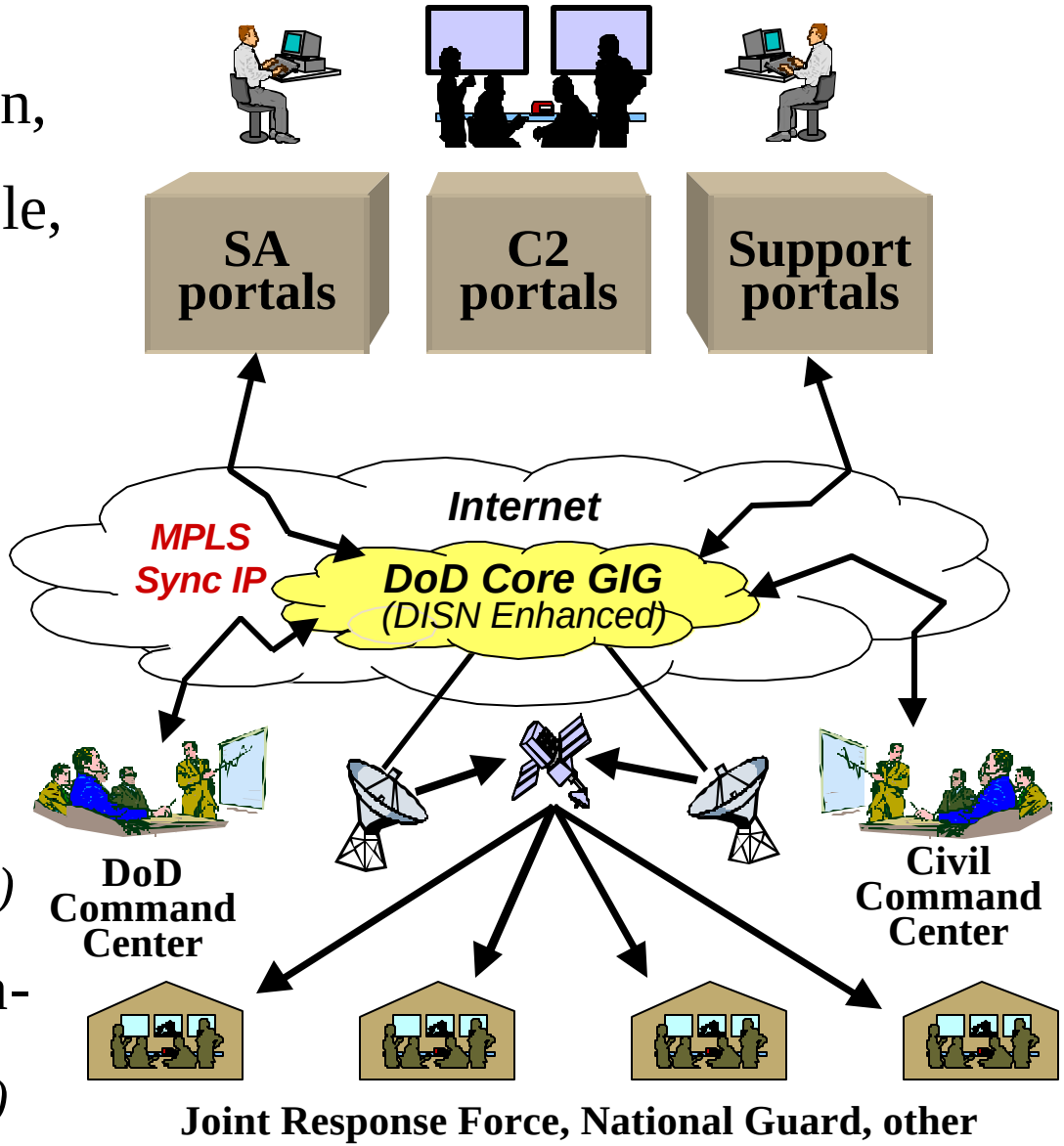
Homeland Defense C2 Nodes & Architecture



Summary: First Technology Challenge

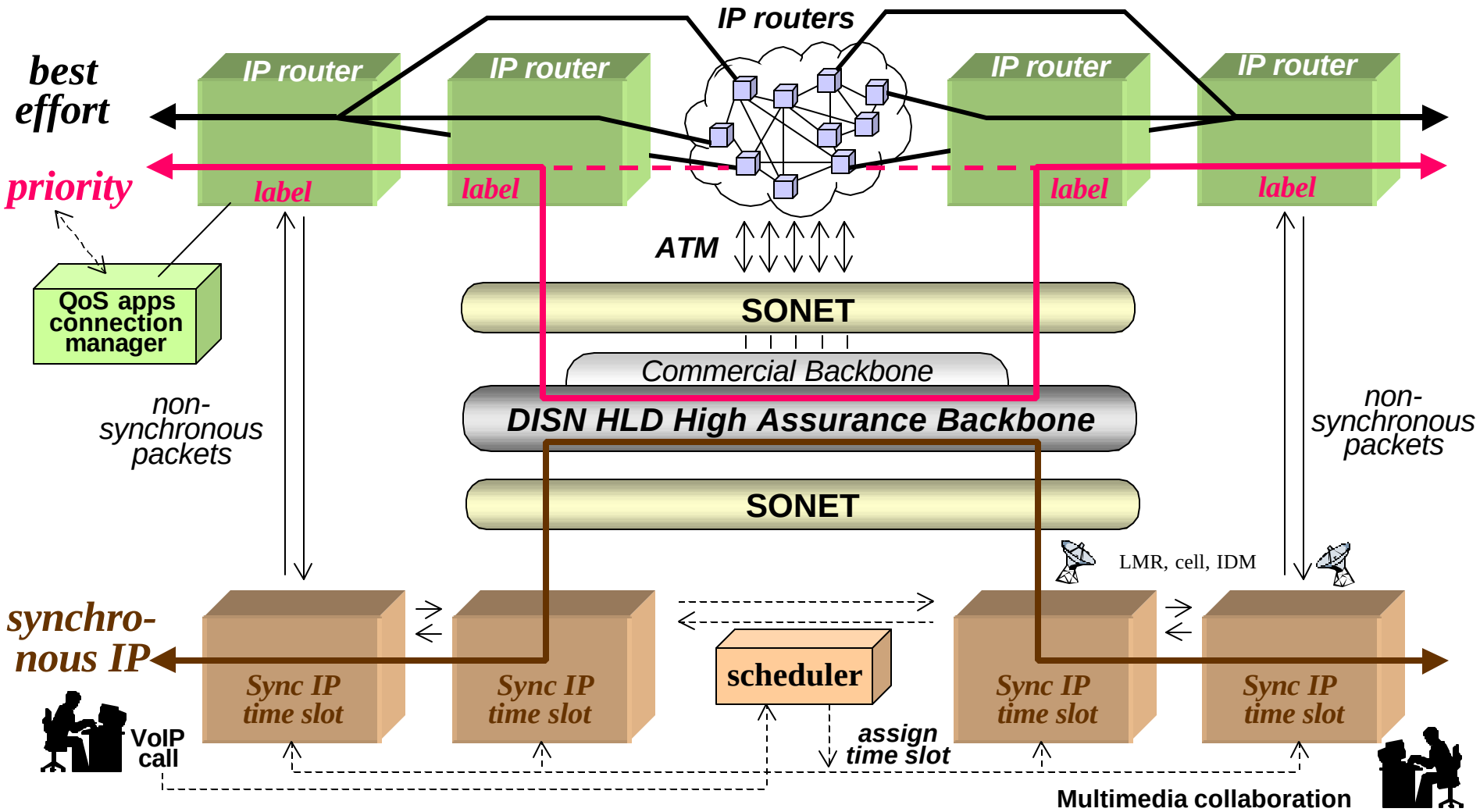
Assured connectivity, situation assessment & coordination

- **Defense-in-depth:**
  - federated, 3rd-generation, bandwidth-adaptive, portal-based, QoS-capable, "push/ pull" architecture
  - a survivable thread of DoD owned & operated backbone … *NSA accredited as part of the GIG!*
  - Assured paths through IP networks based on synchronous & label switched priority routing technologies
  - Land mobile radio *(LMR)* gateways & receive-only satcom portal synchroniza-tion from selected entry points *(next generation IDM)*



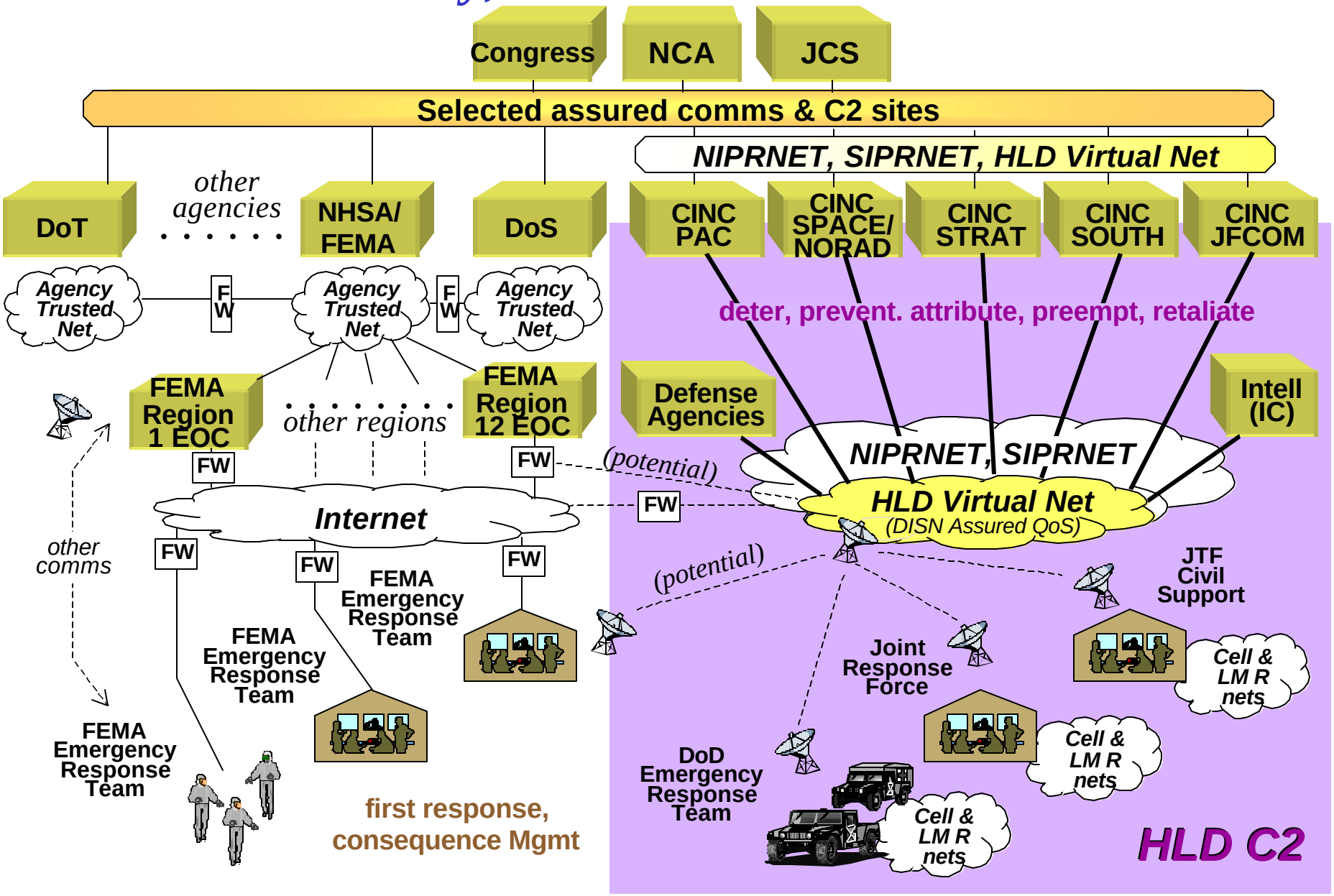
Quality Converged Information Services for Critical Disadvantaged Users

High quality of service data, voice, video, streaming for disadvantaged users



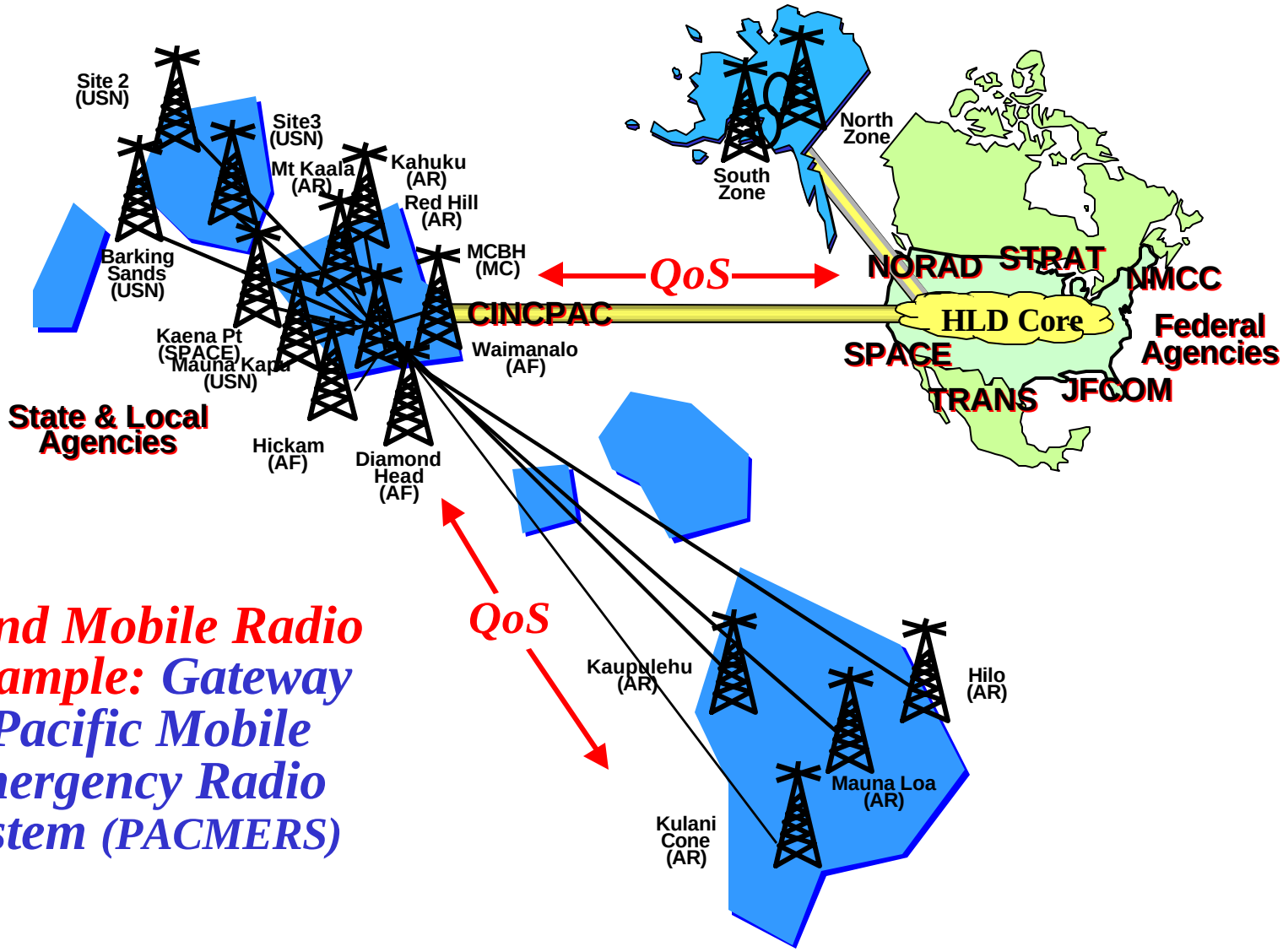
First Technology Challenge

Assured connectivity, situation assessment & coordination



Quality Converged Information Services for Critical Disadvantaged Users

Defense-in-Depth & Redundant Failover of Defense & National Infrastructure



Land Mobile Radio Example: *Gateway to Pacific Mobile Emergency Radio System (PACMERS)*

Second Critical Capability

- **<u>ATTRIBUTION:</u> Capability to assess and track the threat across multiple information domains: and provide high confidence, timely alerts**
  - cyber, terrorist, chem/bio/WMD, air, space, land (& sea)
  - detection, forensics, tracing, correlation
  - legal review

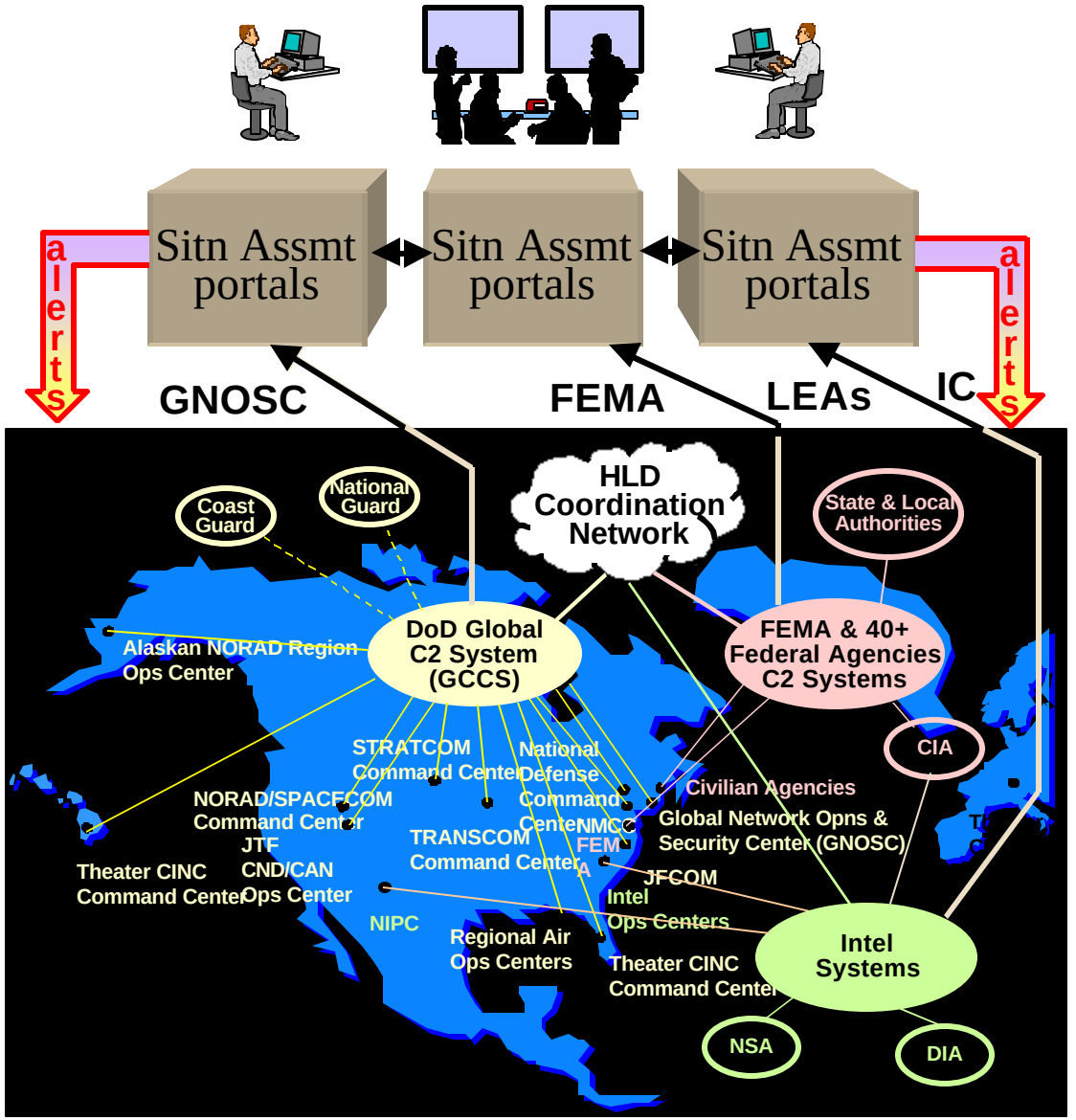
- **Enabling Technology Areas**
  - data mining & correlation tools across cyber, intelligence, law enforcement, & BW databases
  - influence networks for counter-“effects-based operations”
  - new methods of threat visualization & prediction, especially as it relates to critical infrastructure & ops
  - automated alerting & warning using JBI publish/subscribe technology.

Second Technology Challenge

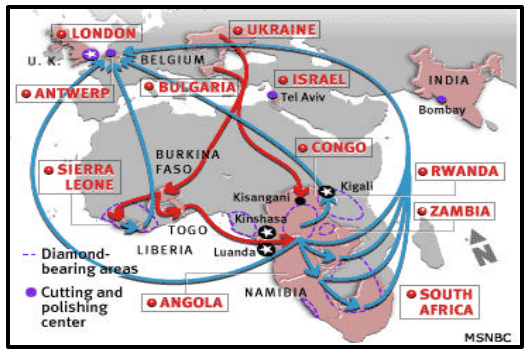
Assessing & tracking the threat across multiple fronts

RT multi-agency collaboration, correlation of cyber to other unconventional threats, I&W

- **Data harvesting, mining, and patterning across cyber, law enforcement, military intel & BW databases**
  - *A quality of cross-correlation so that threats can be localized*
  - *Human factors assessment tools*
  - *Automated foreign lang translators*
  - *Audio/text/video streaming & integration from int. sources*
  - *Cyber attack profiling/patterning*
  - *COA recommendations and dissemination*
- **Decision support grids for ID of targets, pressure points, threat vulnerabilities, threat prediction**
  - *Friendly critical infrastructure influence networks*
  - *RT network activity monitoring*
  - *Single picture big-board visualization*
- **Automated alerting & warning using JBI publish/subscribe technology**
  - *based on USSPACECOM ISC2*



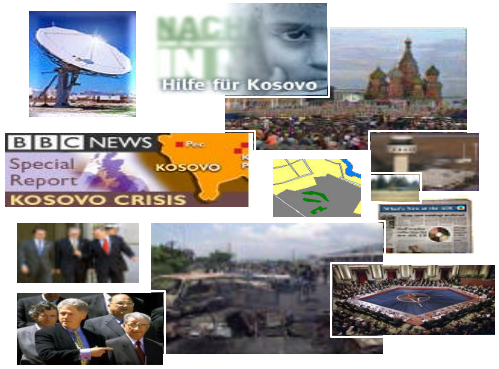
Cross-domain integration of Threat & Vulnerability Assessment Tools



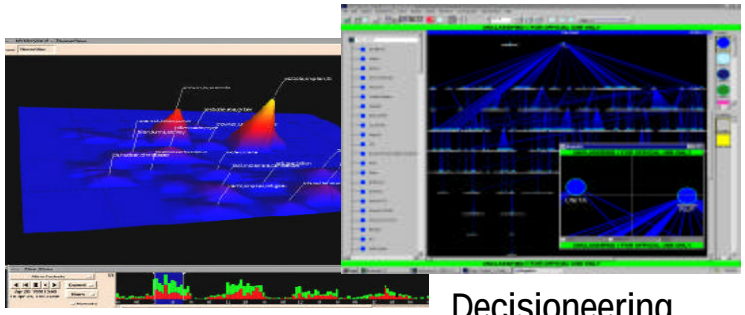
SA (vital threats, players, pressure points, interests)

Legal Review (prior approval to look for bad guys; comply w/ EOs & Regs)

Big-Board Visualization; Collaboration; Mission Planning

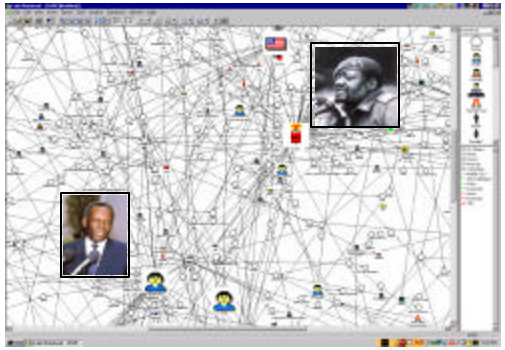


Knowledge Capture (Audio, Imagery, Video, Open Src, Class, English, Foreign)

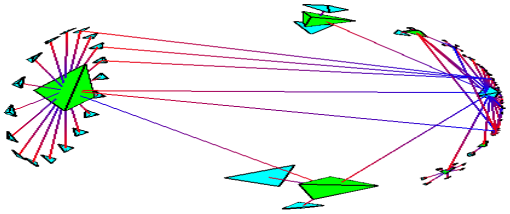


Interactive Data Mining

Decisioneering

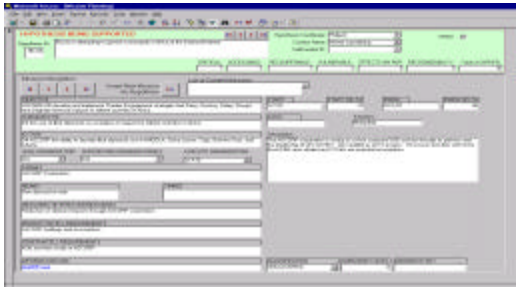


Threat profiling, ethnic & cultural COGs, knowledge maps



Multi-Level Security (MLS)

Foreign Language Translators



Hypothesis creation, analysis, scoring, racking & stacking

Third Critical Capability

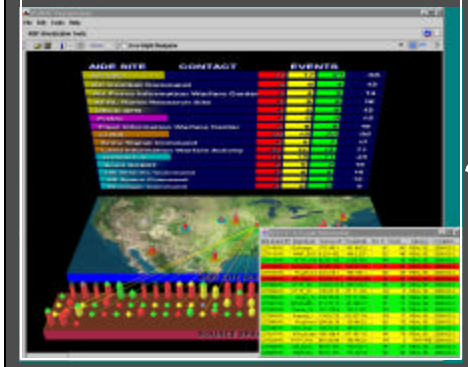
- **CRISIS MANAGEMENT -- *FIRST RESPONSE THROUGH CONSEQUENCE MGMT*:**
  Provide coordinated response to contain/ neutralize threats and recover from damage
  - C2 for CINCs, regional coordinators, incident commanders and first responders … ability to rapidly and reliably transfer/share info with federal, state, local response partners
  - consequence management C2
  - reachback support

- **Enabling Technology Areas**
  - crisis coordination across dissimilar response domains
  - consequence mgmt computational & prediction aids
    - *wrapper technology to integrate legacy & new models*
  - information products compression & realtime services to support warfighter reachback interaction with models, analysts & digital archives. Expansion from CINC 21: collaborative applications as basic web services

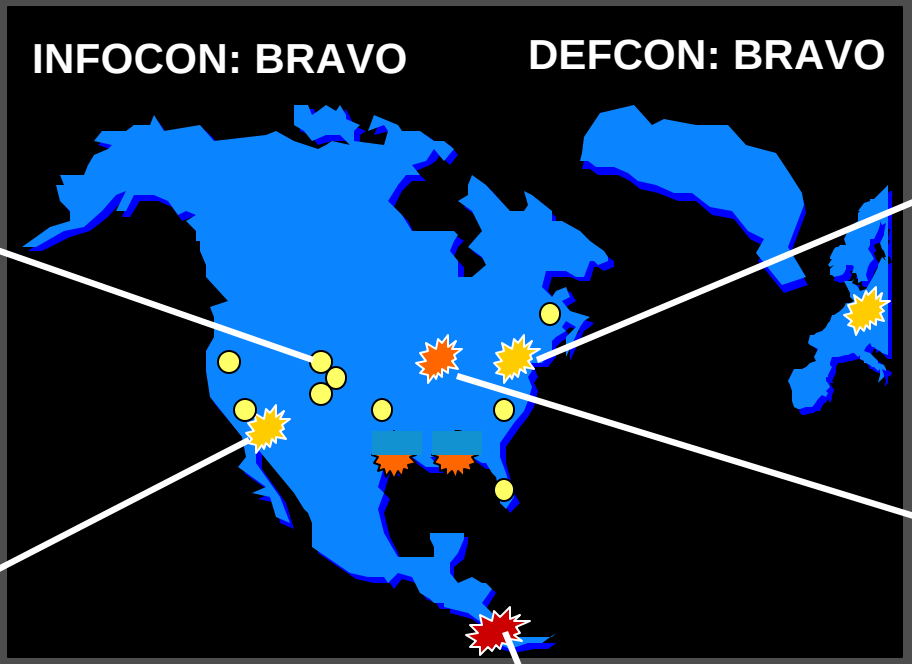
Notional top-level HLD Portal
with drill-down to responders across domains

INDICATORS: *cyber* *terrorist* *coord incident* *WMD* *Air/ Space*

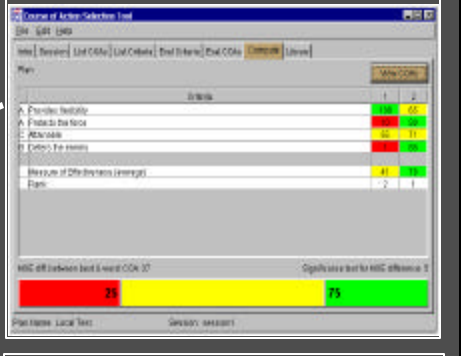
cyber status



INFOCON: BRAVO DEFCON: BRAVO

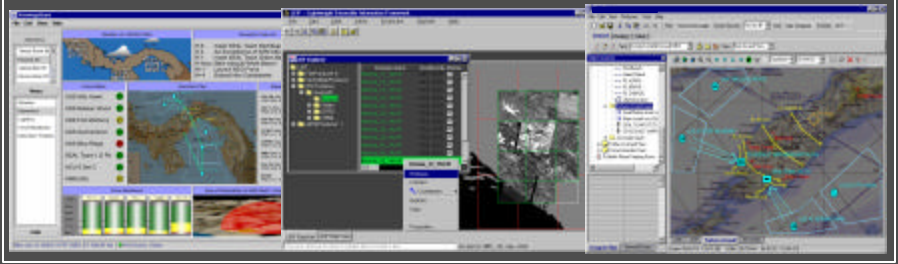


JTF-CS

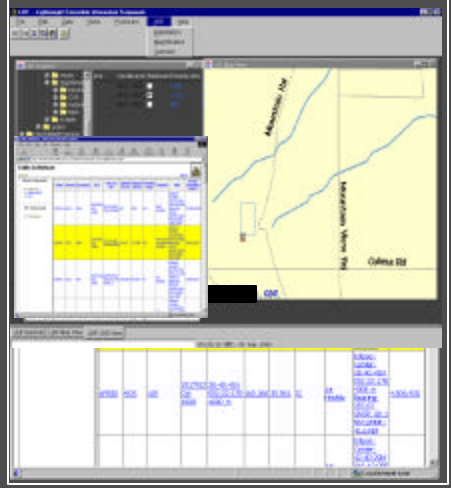


Los Angeles, CA

Canal Zone, Panama

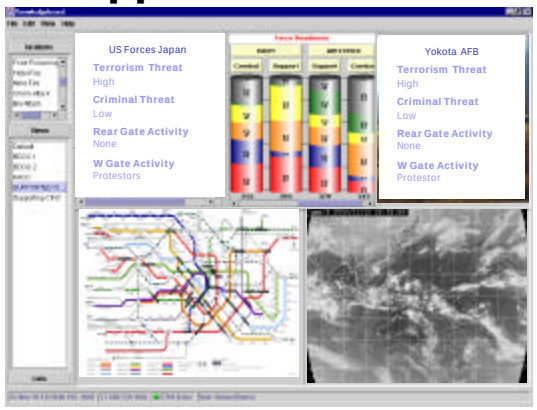


Scott AFB, IL

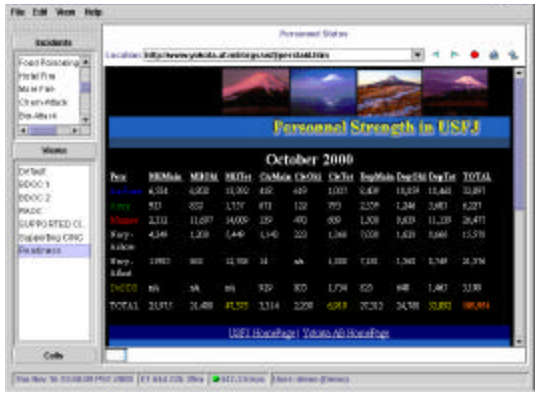


The Response Team Baseline: CRASOC^2 *plus selected tools from DARPA and Services' prototypes*

Supported CINC View

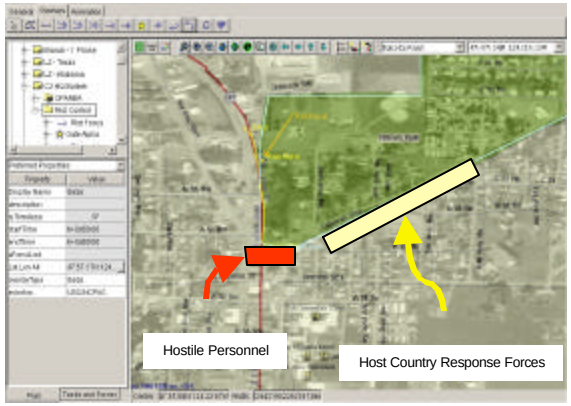


Supported CINC View

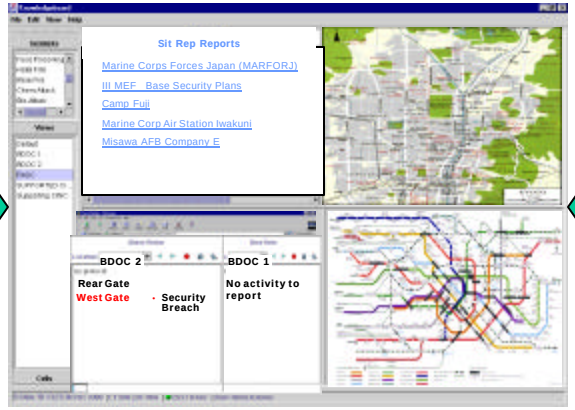


Supporting CINC View

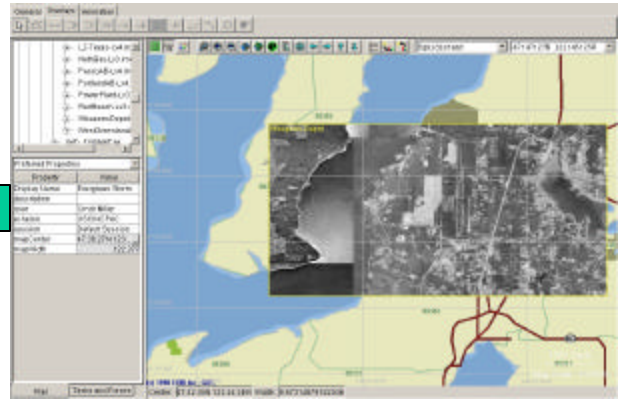
Base 1 Commander's View



Regional Op Center



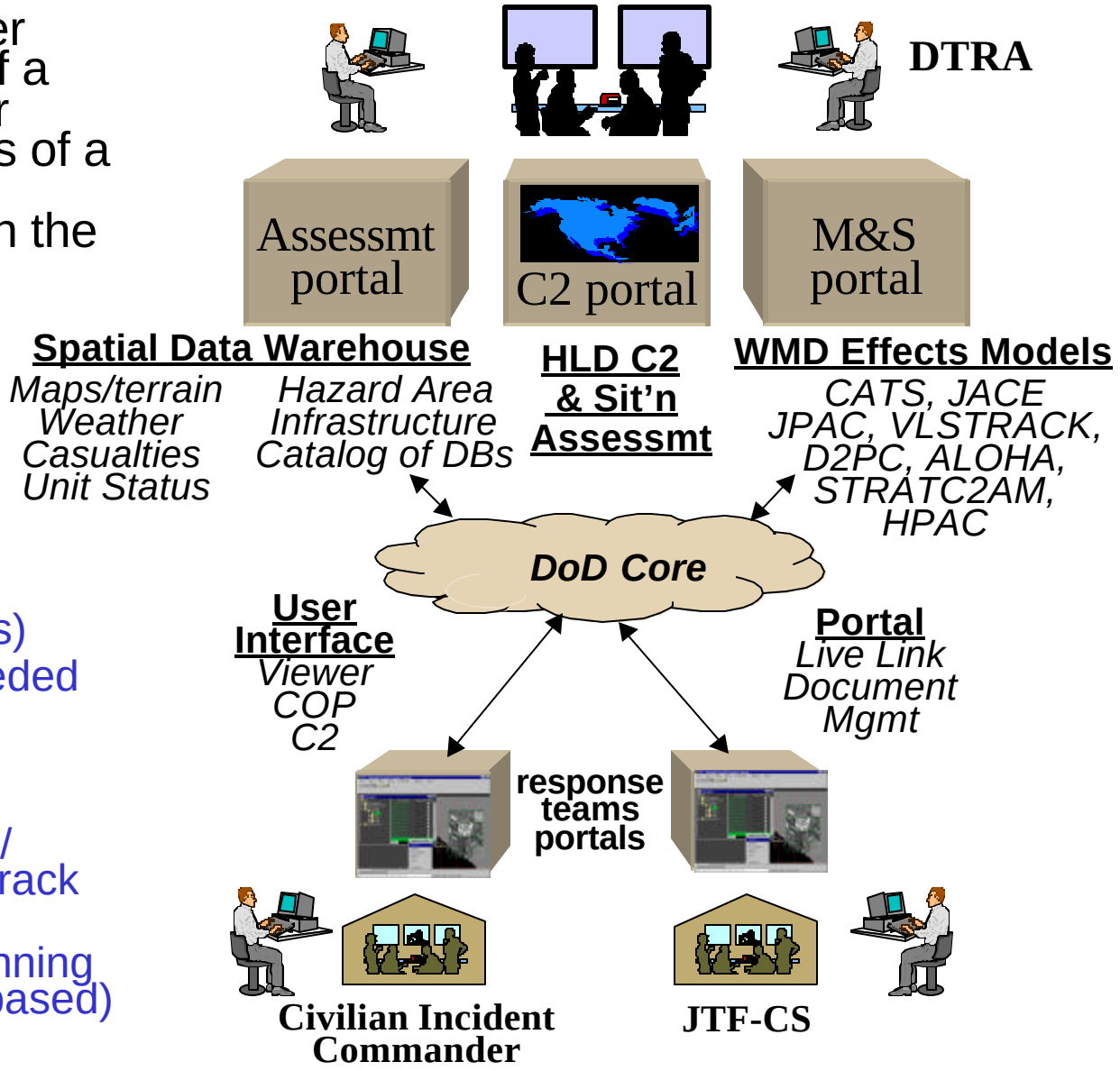
Base 2 Commander's View



Geospatial Force Planning Tool, Knowledge Board, Force Deployment Mgmt Tool, DoD Collaboration Tool Suite, ENCOMPASS, Infrastructure DBs, etc

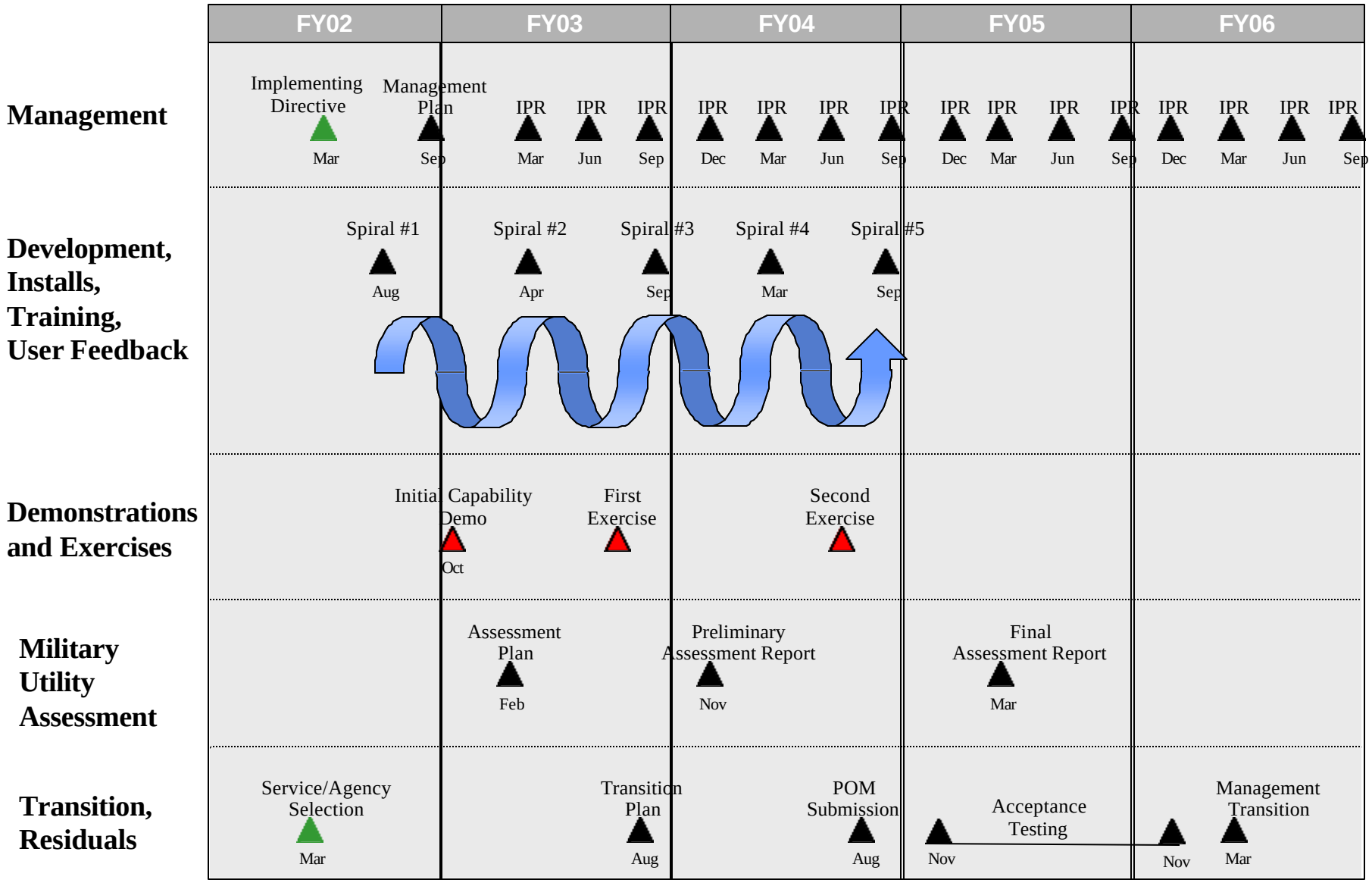
Joint Task Force-Civil Support Conceptual C2 System Architecture

- JTF-CS provides C2 over CoC assets in support of a Lead Federal Agency for managing consequences of a chem, bio, radiological, nuclear, or HE incident in the US, its territories and possessions
- System Tasks:
  - assess situation, share with local response agencies/incident cmdr
  - predict effects/extent & estimate casualties (DTRA/STRAT analysis)
  - estimate resources needed (e.g., med)
  - forces/resource status, infrastructure data
  - mission analysis/COAs/ planning/ assist rqsts/ track task execution
  - training, exercises, planning for CBRNE (template-based)



Demonstrations, Residuals, and Programmatics

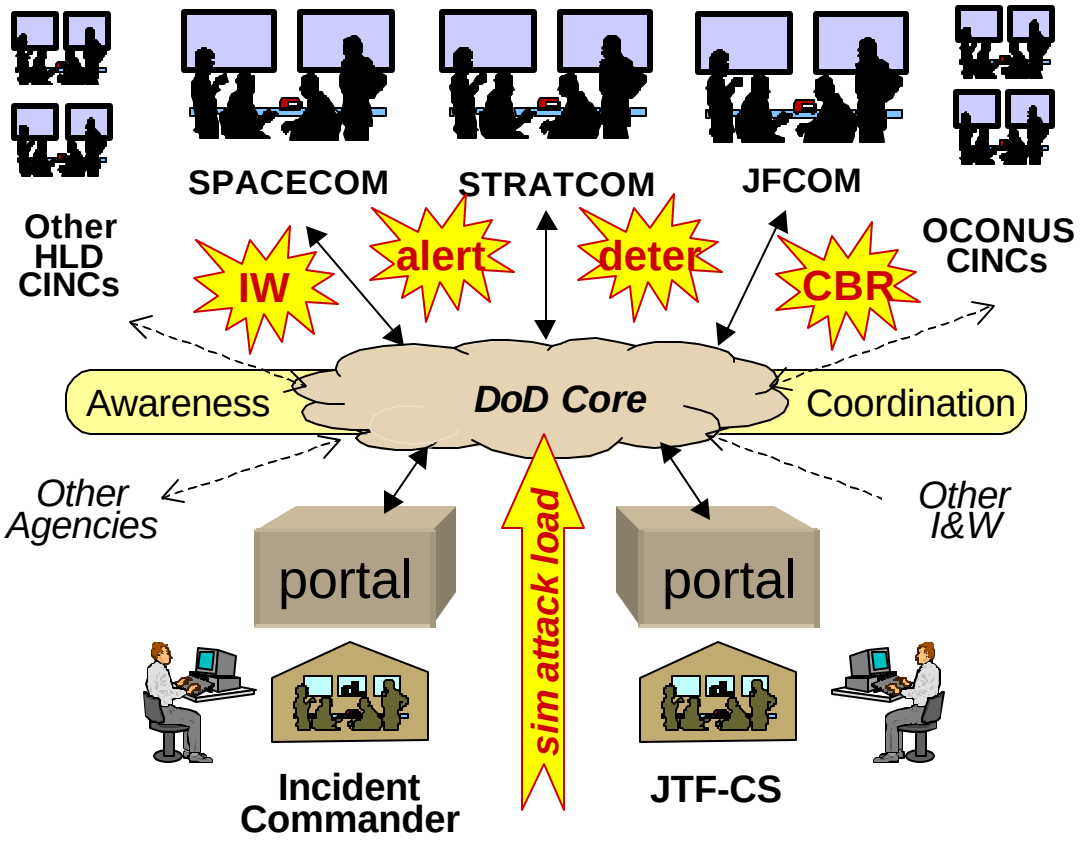
Top-Level Schedule



Homeland Defense C2 ACTD

Demonstrations

- **Year 1:**
  - DoD play, single response team, demo instrumentation *(DISN-LES net)*
- **Year 2:**
  - DoD / Federal Agency play, interagency conops, multi-crisis scenario *(DISN HLD net)*
- **Year 3:**
  - DoD / Federal / State / National Guard play, multiple response forces



Federal Government
- deterrence
- prevention
- preemption
- attribution
- retaliation

State/Local Government
- first response
- consequence management

Private Sector
- cyber defense & response
- bio defense & response

REGIONAL & INCIDENT RESPONSE TEAMS

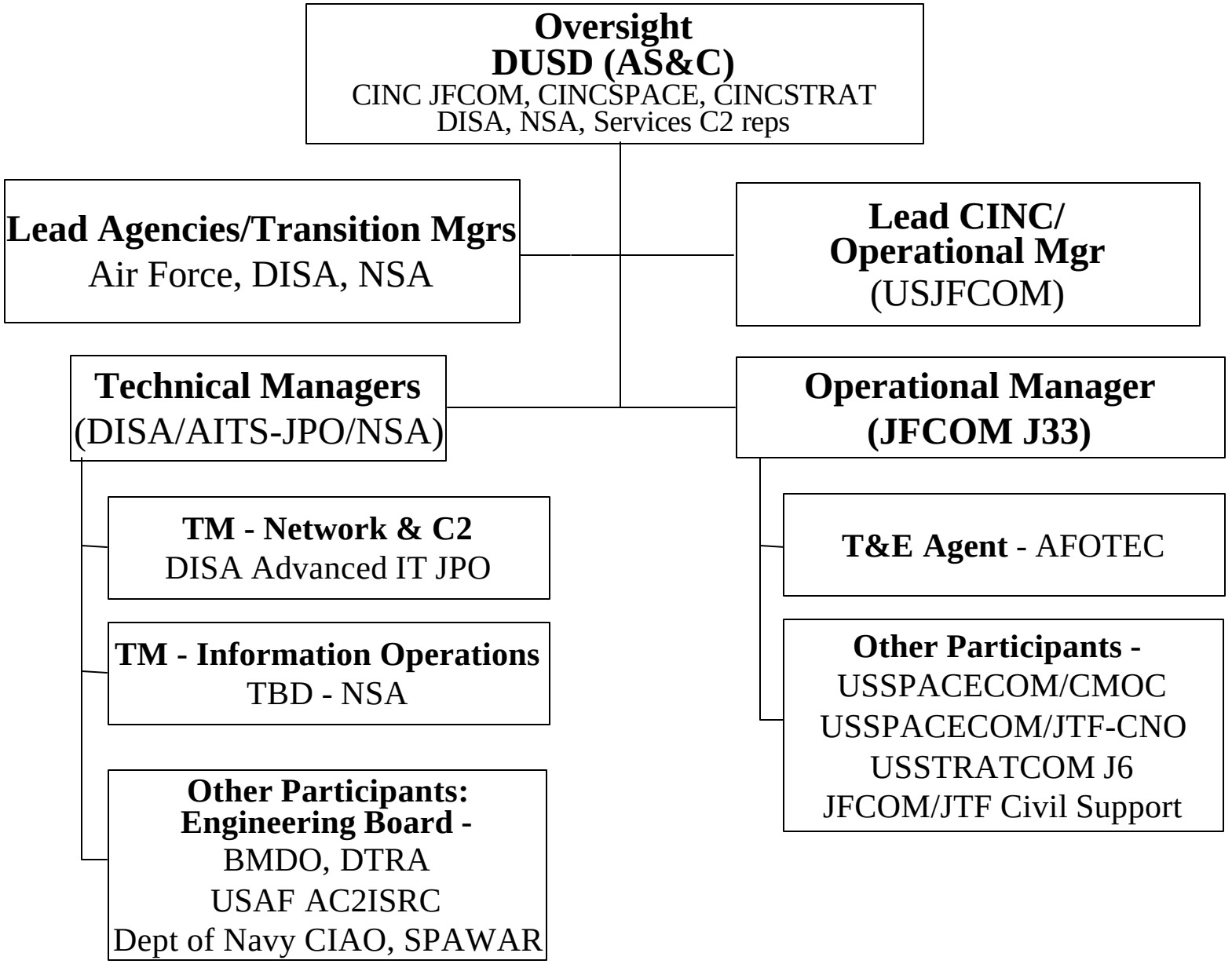
Homeland Defense C2 ACTD

Products & Residuals

- **Residuals**
  - **Network assured delivery and performance for HLD crisis teams via the DISN Core backbone**
  - **HLD Threat Assessment and Response Coordination Software for the IC and DoD** (ICIS, GCCS)
  - **Command Center Capability for Joint Staff or HLD lead CINC** (if identified)
  - **Transportable C2 package for Joint Response Teams** (e.g., JTF-Civil Support)

- **Transitions**
  - **DISA, and Services participants lead DoD HLD C2 technology transition** (e.g., GCCS, DISN, JTF-CS JOC)
  - **NSA lead IC HLD C2 technology transition** (e.g., NSOC, DIA, CIA, JIOC, JWAC)

HLD C2 Project Management



Costs by Capability

	FY02	FY03	FY04	FY05	FY06	TOTAL
•Capability 1 - HLD Network	**$3.0M**	**$2.9M**	**$2.9M**	**$2.0M**	**$2.0M**	**$12.8M**
Network Components	1.0	.9	.9	.7	.7	4.2
Network Engineering	1.0	1.0	1.0	.7	.7	4.4
JTF Comm/LMR gateway	.75	.75	.75	.4	.4	3.05
Demo development	.25	.25	.25			.75
DISN Transition				.2	.2	.4
•Capability 2 - I&W	**$4.5M**	**$4.5M**	**$4.4M**	**$3.0M**	**$3.0M**	**$19.4M**
Threat Tracking Center	1.5	1.5	1.4	1.0	1.0	6.4
Threat Tracking/Alert tools	2.5	2.5	2.5			7.5
Demo development	.5	.5	.5			1.5
IC Community Transition				2.0	2.0	4.0
•Capability 3 - HLD C2/CM	**$3.5M**	**$3.5M**	**$3.5M**	**$2.5M**	**$2.5M**	**$15.9M**
CINC CC Components	1.7	1.7	1.7			5.1
JTF-CS Components	1.3	1.3	1.3			3.8
Demo development	.5	.5	.5			1.5
GCCS/Services Transition				2.5	2.5	5.0
•Network*, Demos, OM Eval	**$0.7M**	**$0.8M**	**$0.9M**	**$0.5M**	**$0.5M**	**$3.4M**
•TOTAL: $51.0M	**$11.7M**	**$11.7M**	**$11.7M**	**$8.0M**	**$8.0M**	**$51.0M**

**includes operating cost for DISN*

Proposed Funding

(in millions)

Organization	FY02	FY03	FY04	FY05	FY06	Total
OSD (DUSD/AS&C)	$ 4.0	$ 4.0	$ 4.0	$ 2.5	$ 2.5	$ 17.0
DISA (AITS-JPO)	$ 2.5	$ 2.5	$ 2.5	$ 2.0	$ 2.0	$ 11.5
NSA	$ 2.5	$ 2.5	$ 2.5	$ 2.0	$ 2.0	$ 11.5
BMDO	$ 0.5	$ 0.5	$ 0.5	$ 0.5	$ 0.5	$ 2.5
AC2ISRC	$ 0.1	$ 0.1	$ 0.1			$ 0.2
Misc Contributions *	$ 2.1	$ 2.1	$ 2.1	$ 1.0	$ 1.0	$ 8.3
Total	$ 11.7	$ 11.7	$ 11.7	$ 8.0	$ 8.0	$ 51.0

* Currently coordinating with DOMS, DON CIAO, SPAWAR, AFRL, DTRA, JFCOM, SOCOM, Army CID/CCIU for $8.3M over 5 years

Total Estimated Project Cost: $51M

Program Risks

- **Technology risks:** **low / med**
  - All components either operational prototypes or pre-production
  - Build upon existing network & C2 infrastructures
- **Program management risks:** **low / med**
  - Numerous communities, participants, stakes, goals, interests, agendas, etc at play
- **HLD Legal and policy risks:** **med / high**
  - ACTD is minimally sensitive to CONOPs chosen
  - Mitigate by addressing at some level but don't dwell
- **Cost and schedule risks:** **low / med**
  - Agencies will manage own pieces to product delivery
  - Network configuration will be limited by op costs. Core network availability being negotiated with DISA NS

Why is this ACTD important?

- Everything here will help ensure our connectivity between DoD CONUS resources, plus reachback support connectivity to Overseas CINCs
  - *Most of DoD's networks are built on the vulnerable, commercial infrastructure !!!*
- The capabilities will be valuable to warfighters **at home and abroad**, even while the debate on policy development and organizational control for "homeland defense" continues
  - e.g., natural disaster response coordination
  - e.g., USSPACECOM assured warning dissemination
  - e.g., USSTRATCOM assured EAM dissemination
  - e.g., cross-domain threat warning & attribution in the IC

Payoffs & Summary

- This ACTD will demonstrate:
  - An assured way to dynamically redistribute DoD's critical information flows in a crisis
  - A first cut at capability to execute a new complex, cross-mission-area, multi-threat, coordinated national operation
  - Greater confidence in continuity of disbursed operations in the kind of crisis that we have never seen before!
- The threat is unpredictable, but prudent preparedness says that some coordinated nation-state or terrorist attack is highly likely to happen in the next decade
  - This ACTD will take 3 years to capability demo and at least 5 years to production
  - That is the median expected date for something to happen . . .

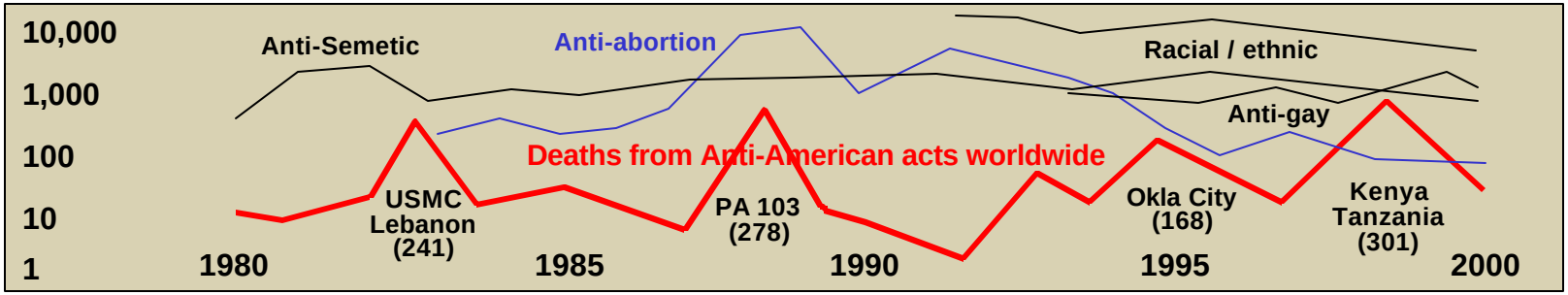
Questions?

"Only the dead have seen the end of war" *- Plato, circa 500 B.C.*

BACKUP SLIDES

Terrorism against U.S. citizens

- 250,000-300,000 terrorist acts against Americans worldwide over the past 20 years
  - Fewer than 3,000 committed abroad
  - 1,500 Americans have died in unpredictable incidents -- mostly bombings (600 in Lebanon Marine barracks and Pan Am 103)
- Political beliefs have little to do with domestic terrorism
  - largest categories are racial/ethnic crimes, religious, and anti-gay. Many were spur-of-the-moment acts
  - 12,000 anti-abortion incidents from 1984-2000
  - no statistics on other types (e.g., high school shootings, civilian/police violence)



* Rodger Doyle, "The Americal Terrorist", Scientific American, June 2001

Considerations for a Presidential Action Plan

- **Threat of asymmetric attacks** on American homeland, either by nation-states or terrorist organizations, is real and will increase during the next decade
- **Federal government** will play the leading role in deterrence, prevention, preemption, attribution, and retaliation
- **State and local government** assets (incl National Guard) will play the lead role in first response and consequence management
- **Private sector** will play a critical operational role, particularly in defending against and responding to cyber and biological attacks
- An **integrated warning/information/coordination system** is required to ensure effective use of resources to mitigate effects during and after large-scale attacks or campaigns

Col Randall Larsen & Dr. Ruth David, "Strategic Review", Fall 2000 edition

National Defense Panel, Dec '97
"National Security in the 21st Century"

- **A Transformation Strategy for the Unified Command Plan**
  - Four (vice current five) geographic Unified Commands:
    - **Americas Command** (incl SOUTHCOM, Homeland Defense Command, and NORAD) includes all Americas & U.S. ocean approaches and assumes Military Support to Civil Authorities (MCSA) role from Army.
    - **EUCOM** extended to included Russia & other former Soviet, Egypt, Jordan, Sudan; **PACOM** assumes responsibility for Pakistan; **CENTCOM** focus on oil sources of Persian Gulf & Caspian Sea -- gives up the above states and adds former Soviet Caspian Sea area states STRATCOM, SOCOM continue current responsibilities
  - JFCOM is common force provider (active & reserves) to all other commands; develop & validate Joint Doctrine; conducting & overseeing all joint/combined experimentation. Gives up conflicting role as supported CINC (to NATO)
    - CINCLANTFLT becomes SACLANT
  - LOGISTICS COMMAND would provide global logistics, transportation & asset visibility operations … focus on rapid force projection with smaller footprints & leverage industry innovations & practices.
    - TRANSCOM plus DLA
  - SPACECOM provides global awareness, space ops, information superiority, and manages global information infrastructures for the geographic commands
    - subsumes DISA

Hart/Rudman Commission, Jan 31, 2001

"*Roadmap for National Security: Imperative for Change*"

- **Recommend create a National Homeland Security Agency (NHSA) with Cabinet status**
  - plan, coordinate, integrate U.S. Government activities involved in homeland security
  - built on FEMA, with the three border security organizations transferred to it (Coast Guard, Customs, Border Patrol)

- **New priorities for the U.S. Armed Forces**
  - Replace "two-major-conflict" force structure planning with "one-major-conflict plus homeland defense plus smaller contingencies"
  - National Guard be given homeland security as a primary mission per the U.S. Constitution *(natural, manmade, and/or WMD-triggered disasters)*
  - Other forces are "homeland security" (reserves plus active forces augmentation supporting NHSA), "strategic nuclear", "expeditionary"* (rapid, light deployment), "conventional", or "humanitarian"
  - Unify Space: transfer DoD "Space Architect" to NSC staff to lead
  - Faster response to threat: employ a "two-track" acquisition system -- one for major acquisitions and a second "fast track" for a limited number of potential breakthrough systems, especially in the area of C2
    - *Foster innovation by directing a return to the pattern of increased prototyping and testing using broad industrial base vice "defense industry"*

* *highest priority for DoD forces*

Background

- **The United States military has a long history of providing support and assistance to domestic civil authorities during emergencies and other instances of national concern.**
  - **Assists relief agencies during natural disasters**
  - **Provides counterdrug support to federal law enforcement agencies**
  - **Logistics, Security, and Consequence Management support to Civilian Authorities during High Vis special events.**
- **Civilian relief or law enforcement officials remained firmly in charge.**

Background cont.

Presidential Decision Directive 39

- **Defines the United States policy on counter-terrorism.**
- **The intent is to deter, defeat, and respond vigorously to all terrorist attacks on U.S. territory and against our citizens, or facilities, whether they occur domestically, in international waters or airspace, or in foreign territory.**
- **The U.S. shall have the ability to respond rapidly and decisively to terrorism directed against us wherever it occurs, to protect Americans, arrest or defeat the perpetrators, respond with all appropriate instruments against the sponsoring organizations and governments and provide recovery relief to victims, as permitted by law.**

Department of Defense's Role

DOD directives 3025.15 and 2000.12 and the Chairman Joint Chiefs of Staff CONPLAN 0300-97, and on approval by the Secretary of Defense, will provide assistance to the LFA and or the CONPLAN Primary agencies, as appropriate, during all aspects of a terrorist Incident, including both crisis and consequence management.

DOD serves as a support agency to:

- Crisis Management: FBI for technical operations.
  - TEU
  - EOD
- Consequence Management: FEMA for support operations.
  - JTF/CS
  - CBIRF
  - SRTs
  - NGCST

Inter-agency CONOPs for Homeland Natural Disaster Response

the FEMA "Federal Response Plan"

National Level Actions

Establish Catastrophic Disaster Response Group & Agency Emergency Support Teams

Activate ESFs (as required)

Activate Agency EOCs

Regional Level Actions

Establish Regional Op Center

Deploy Advance Element of Emergency Response Team (to State Op Facs & disaster site)

Establish Disaster Field Office

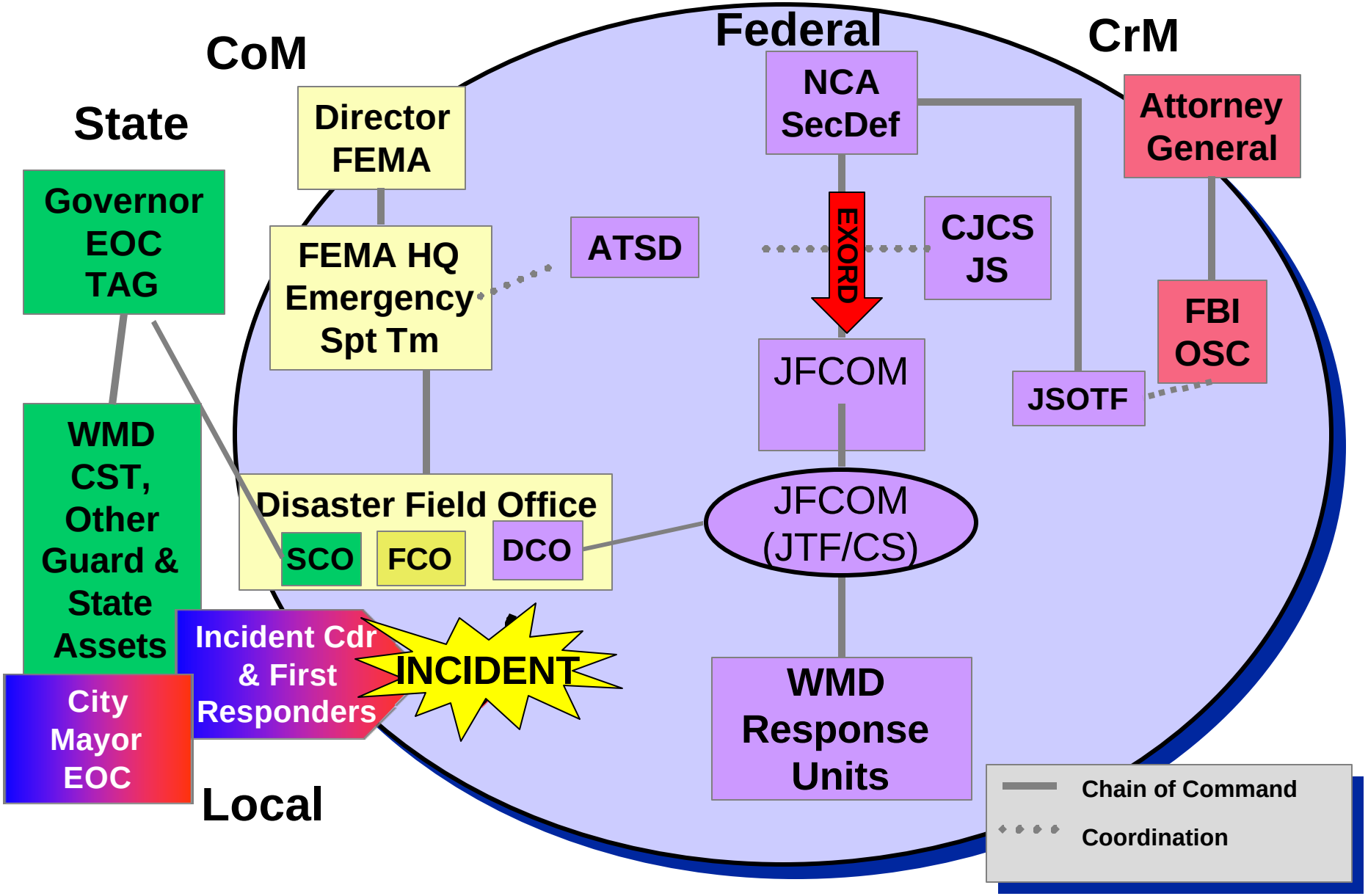
Respond with Full Emergency Response Team

Emergency Support Functions (ESFs)

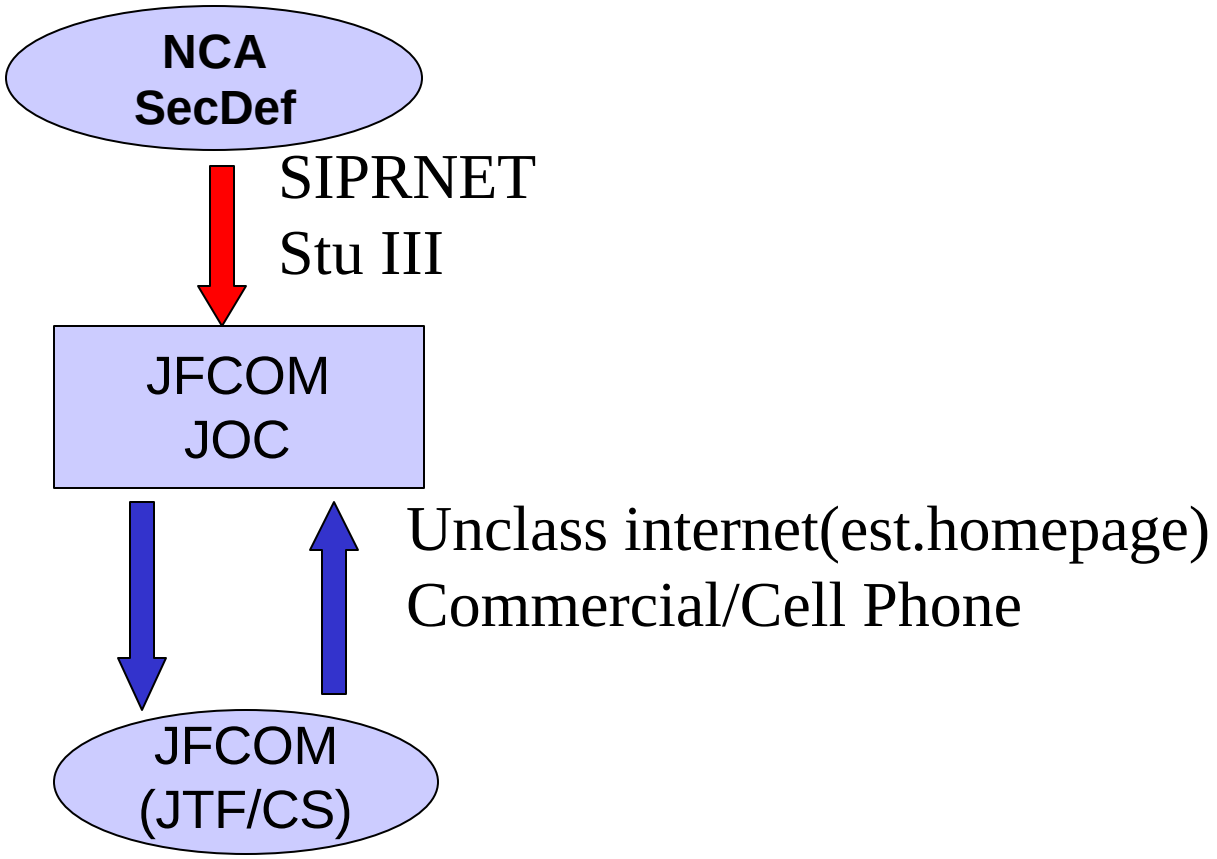
ESF \ Dept or Agency	USDA	DIC	DOD	DOEd	DOE	DHHS	DHUD	DOI	DOJ	DOL	DOS	DOT	TREAS	VA	AID	ARC	EPA	FCC	FEMA	GSA	ICC	NASA	NCS	NRC	OPM	TVA	USPS
Transportation	S		S		S						S	P								S	S					S	S
Comms	S	S	S					S										S	S	S			P				
Public Works & Engineering	S	S	P		S	S		S		S		S		S			S			S						S	
Firefighting	P	S	S					S									S		S								
Information & Planning	S	S	S	S	S	S		S	S			S	S			S	S		P	S		S	S	S			
Mass Care	S	S	S			S	S					S		S		P			S	S							S
Resource Support	S	S	S		S	S				S		S		S					S	P			S		S		
Health & Medical Svcs	S		S			P			S			S		S	S	S	S		S	S			S				S
Urban Search & Rescue	S		P			S				S		S			S		S		S	S							
HazMat	S	S	S		S	S		S	S	S	S	S					P		S	S				S			
Food	P		S			S						S				S	S		S								
Energy	S		S		P						S	S								S			S	S		S	

P = Primary responsibility, S=Support

Chain of Command



Conductivity



- BSI can support SIPRNET and Stu III capability if available
- Not deployable to the incident site

Military Need

- Ability to rapidly and reliably transfer/share information with response partners
  - Local
  - State
  - Federal
- Compatible communications infrastructure
  - Non-Secure
  - Secure link

USCINCJFCOM's JOC focal point for coordination of requested DoD support to Civilian Authorities

First Technology Challenge

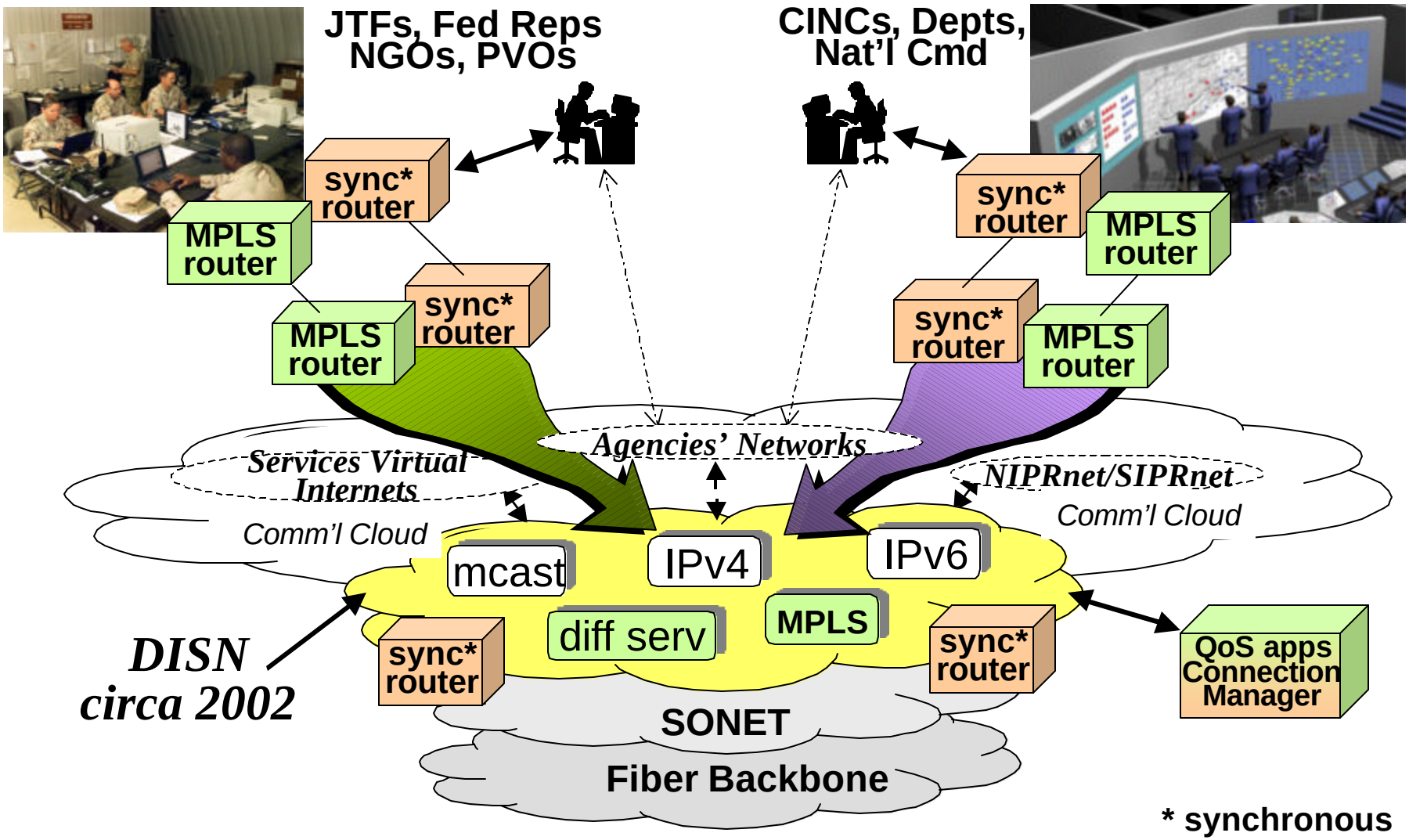
Related NCS Efforts and a potential transition

- Classified programs exist to assure voice/data connectivity to selected government & military personnel during National Security & Emergency Preparedness activities (e.g., SRAS, CWIN*)
  - » *they are point-to-point voice / data (64kbps)*
  - » *none directly address multipoint or multicast IP network traffic*
  - » *there is **no** accessible, inter-ISP QoS capability in the Internet*
- Results of the ACTD can serve as risk reduction for NCS's negotiations with NSPs/ISPs for a standards-based assured Internet capability … and for the Services Virtual Intranets

* *Special Routing and Access Service, Cyber Warning Information Network*

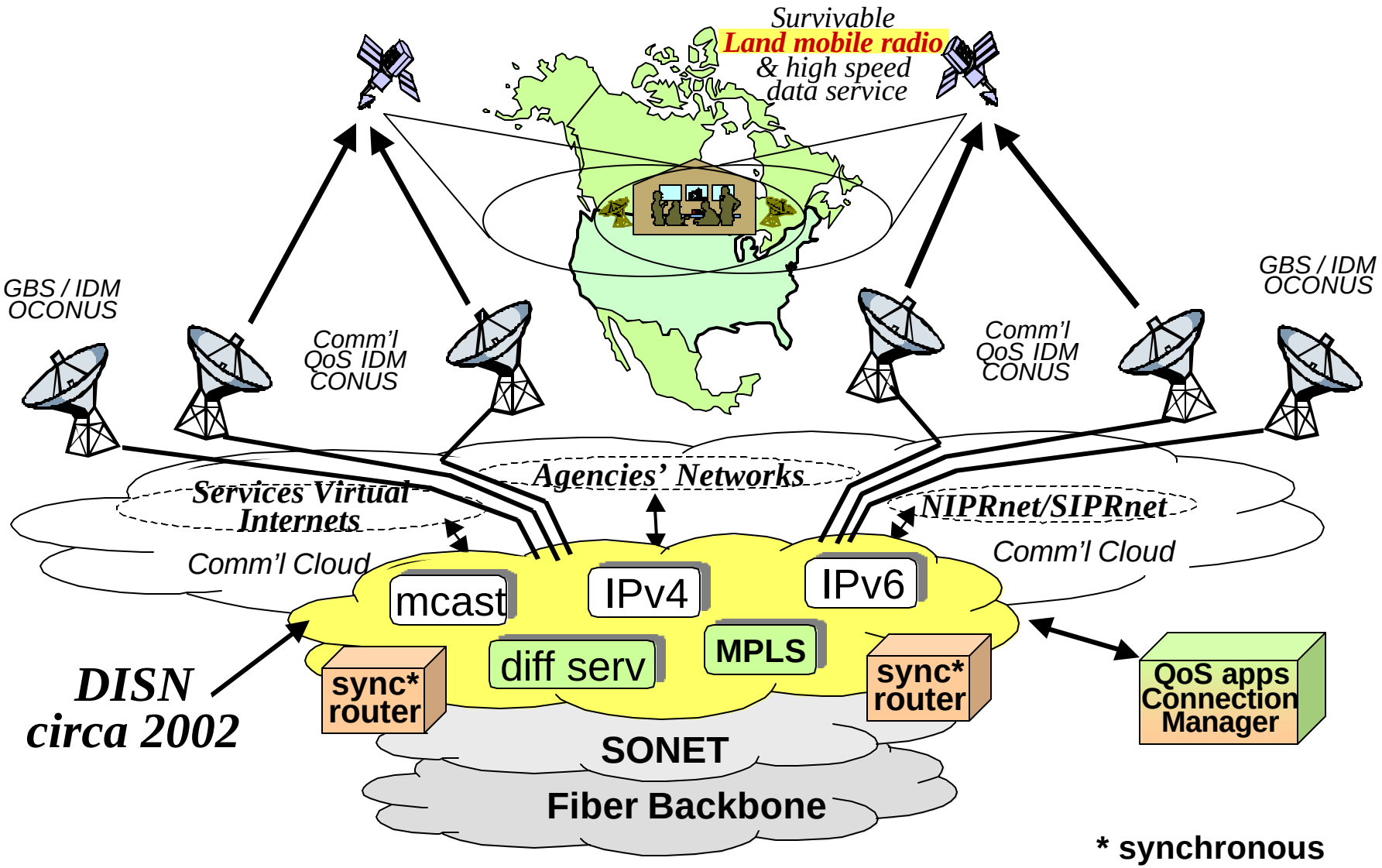
Quality Converged Information Services for Critical Disadvantaged Users

High quality of service data, voice, video, streaming for disadvantaged users



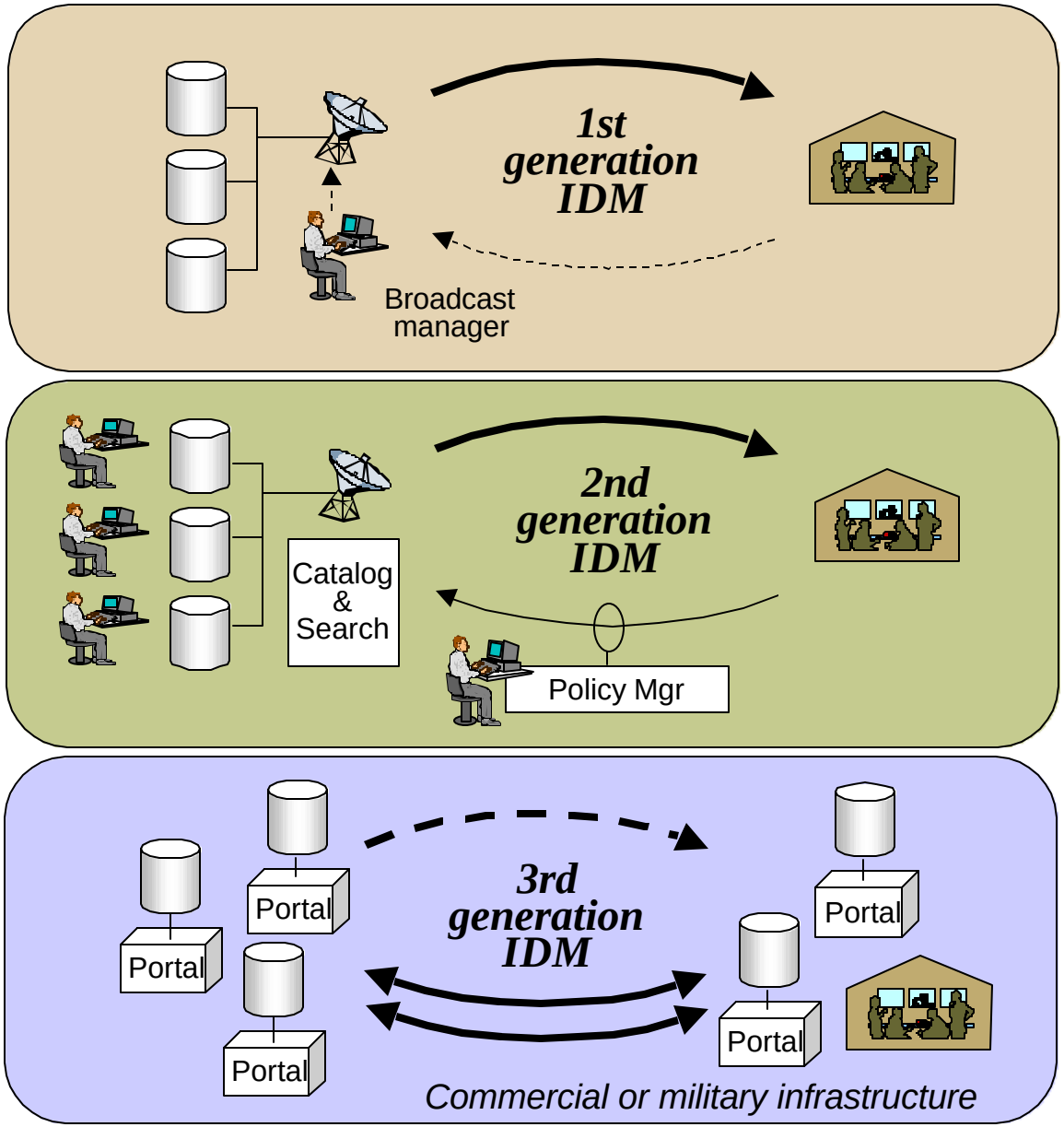
Quality Converged Information Services for Critical Disadvantaged Users

Defense-in-Depth & Redundant Failover of Defense & National Infrastructure



Assured connectivity, situation assessment & coordination

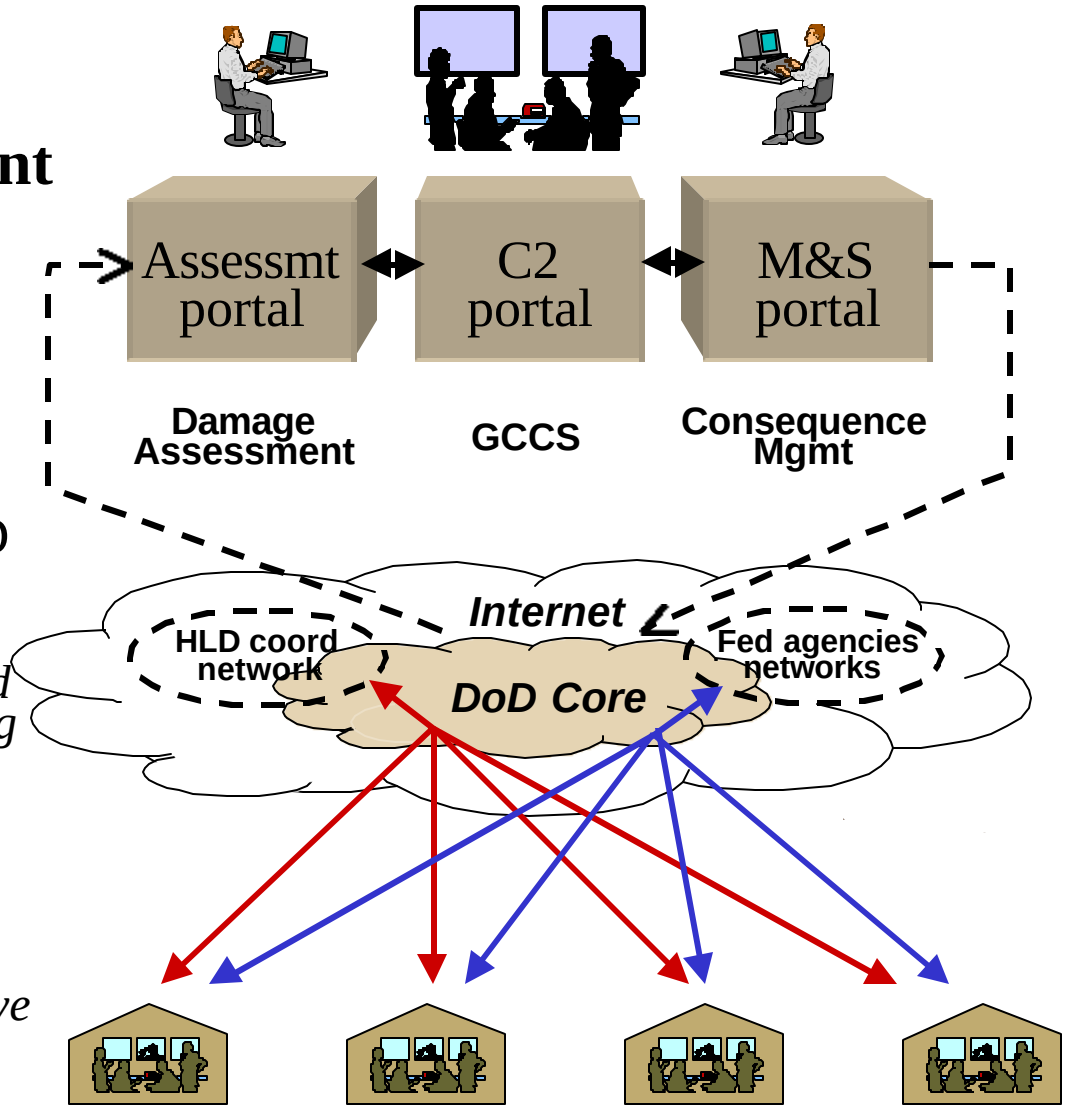
- **3rd-generation Portal-based, decision-centric virtual workspaces**
  - single sign-on
  - personalization
  - content management
  - federated, cooperating portals
  - distributed collaboration
  - format adaptation (including security, language translation)
  - load-balancing & bandwidth adaptive distribution
  - traffic analysis
  - content adaptation to patterns, users



Third Technology Challenge
Consequence Mgmt Computational & Prediction Aids

- **CRASOC2 Portal as a base capability**
- **Consequence management computational and prediction aids:**
  - Realtime, online modeling by DTRA or other supporting analysis centers
  - Blue force C2 vulnerability & response models for DoD HLD operations

  ("operational" & "tactical" portions which are not defined today, integrated with existing classified strategic models)
- **Rapid response team reachback to HLD - relevant information**
  - *bandwidth and content-adaptive portal-to-portal push, pull & streaming*
  - *auto-compression*



MOPs & MOEs

MOEs for HLD C2 infrastructure: how well does HLD C2 infrastructure...

- move and share information easily across protected boundaries/multiple enclaves?
- Provide adequate security and monitoring across protected boundaries/enclaves?
- Increase multi-user multi-community HLD C2 network utility?
- Provide for easy monitoring and readjustment of QoS and QoS policies during multiple, simultaneous crisis events?
- Resist performance degradation to most important crisis responders and reachback sites during sever network disruption from attack and crisis-induced user surge?

MOPs for Threat Assessment and Analysis tools:

- Are tools (eg, collaboration, threat profiling, data mining & patterning, etc) across multiple HLD communities interoperable, scalable, portable?
- Do tools improve/enhance integration of data from disparate sources?
- Do tools provide information and situation awareness in a more “operational” sense?
- Do tools provide accurate and adequate cues and alerts across communities?
- Do tools provide improved operator situational understanding, productivity?

MOPs for HLD C2 tools:

- Are tools provide information and visualization to permit seamless coordination of operations from the incident scene(s) up through multi-CINCs, multi-Agencies
- Do tools provide accurate and adequate cues and alerts across communities?
- Do tools provide improved deployed operator productivity through reachback?
- Do tools improve decision making capability and productivity?
- How well do tools allow HLD mission/status and performance to be visualized ?

What technology will we have when we are done?

High-assurance, attack-resistant backbone:

The Defense Information Systems Network (DISN) has added a very high performance, high integrity, IPv4/6 backbone in CONUS that is just becoming operational. We can create a HLD subnet on the core.

Opportunity to activate diverse, dynamic, assured Quality of Service (QoS) over fixed or mobile infrastructure

Guarantees low latency jitter in highly congested networks (up to 90%) to support reliable real-time data streams and voice over IP

Next Generation Information Infrastructure for Coordinated Response

Enhanced Commercial/DOD interoperability for mobile services (voice, message, stream, web) for MSS, LMR, 3G Wireless

Software Defined Radios tied to information control mechanisms

Flexible Information Manipulation for Visualization

Threat Assessment and Analysis Tools